Data Protection

Manual of Guidance Part 1: Standards

Version 3.0 – Approved by the ACPO Data Protection, Freedom of Information and Records Management Portfolio on 25th February 2010

Replaces Version 2.0 (Approved at the ACPO Data Protection, Freedom of Information and Records Management Portfolio on 26th February 2009)

This manual may be disclosed to the public in its entirety

This manual has been produced by the Association of Chief Police Officers (ACPO) Data Protection, Freedom of Information and Records Management Portfolio Group on behalf of ACPO. It is updated and adapted to reflect decisions made by ACPO, views of the Information Commissioner (where appropriate) and the evolution of the legislation as it is interpreted, challenged or reviewed. All modifications to this manual will be the responsibility of the ACPO Data Protection, Freedom of Information and Records Management Portfolio Group.

All enquiries about this manual should be addressed to the Secretary of the ACPO Data Protection, Freedom of Information and Records Management Portfolio Group.

Acknowledgements

ACPO would like to express its thanks to Andy Begent, Essex Police, and colleagues who have assisted in the creation of this Manual.

ACPO, 1st Floor, 10 Victoria Street, London SW1H 0NN

Contents

Contents **3**

Preface **7**

1 Responsibilities and Structures **8**

1.1 Overview 8
1.2 Responsibilities 8
1.2.1 Chief Officer – Data Controller 8
1.2.2 Senior Manager 8
1.2.3 Senior Information Risk Owner (SIRO) 9
1.2.4 Data Protection Officer 9
1.2.5 Senior Responsible Officer (SRO), Senior System Owner (SSO) and Information System Owner 10
1.2.6 All Staff 10
1.3 Structure 11
1.4 Data Protection Training and Awareness 11
1.5 Publication of Data Protection Guidance 11
1.6 Data Protection Compliance Auditing, Data Quality Auditing and Monitoring 11
1.7 ACPO Data Protection Portfolio 12
1.7.1 Appointment of Portfolio Holder 12
1.7.2 Portfolio Group Terms of Reference and Structure 12
1.8 Standards 12

2 The Police, Processing and Principles **13**

2.1 Overview 13
2.2 Compliance with the principles 13
2.3 Processing of personal data by the police 14
2.4 The use of de-personalised information 14

3 Fair and Lawful Processing **16**

3.1 Overview 16
3.2 The First Principle 16
3.2.1 First Principle: Introduction 16
3.2.2 First Principle: Lawful Processing 16
3.2.3 First Principle: Fair Processing 18
3.2.4 First Principle: Schedule 2 ('Legitimate Processing') Conditions 21
3.2.5 First Principle: Schedule 3 (Sensitive Personal Data) Conditions 24
3.3 The Second Principle 28
3.3.1 Second Principle: Introduction 28
3.3.2 Second Principle: Notification 28
3.3.3 Second Principle: Incompatible Use 29
3.4 Disputes and Complaints 29
3.5 Fair & Lawful Processing: Checklist 29
3.6 Standards 30

4 Privacy Impact Assessments (PIAs) **31**

4.1 Overview 31
4.2 Privacy Impact Assessments 31
4.2.1 Assumptions 31
4.2.2 Recommendations 31
4.2.3 Introduction 31
4.2.4 What are Privacy Issues? 31

4.2.5 Key Messages about PIAs 32
4.2.6 Why undertake a PIA? 32
4.2.7 Do all IT new process/initiative/IT systems require a full PIA? 32
4.2.8 When should a PIA be undertaken? 32
4.2.9 Examples of new initiatives/IT systems 33
4.2.10 What should a PIA document look like? 33
4.2.11 Who should conduct a PIA and who should be involved in the process? 33
4.2.12 Consultation 33
4.2.13 Responsibilities 33

5 Data Quality, Review, Retention and Disposal 47

5.1 Overview 47
5.2 Data Quality 47
5.2.1 Introduction 47
5.2.2 Third Principle 47
5.2.3 Fourth Principle 48
5.3 Review, Retention and Disposal 50
5.3.1 Fifth Principle 50
5.4 Disputes and Complaints 51
5.5 Checklist 51
5.6 Standards 52

6 Subject Access 53

6.1 Overview 53
6.2 Right of Subject Access 53
6.3 Subject Access Procedure 54
6.4 ACPO Standard Application Form 54
6.5 'National' and 'Local' Applications 55
6.6 'Satisfactory' Applications 55
6.6.1 Fee 55
6.6.2 Identification 55
6.6.3 Sufficient Information 56
6.6.4 Applications made on behalf of another – Agents/Power of Attorney/Persons with Disabilities 56
6.6.5 Applications made on behalf of another – Young Person 57
6.6.6 Repeated Applications 57
6.7 Circumstances when information and personal data may be withheld 57
6.7.1 Third-Party personal data 57
6.7.2 Disproportionate Effort 58
6.7.3 Subject Access Exemptions 58
6.7.4 Information other than Personal Data or Third-Party Personal Data 63
6.8 Other considerations 63
6.8.1 Routine Amendment and Deliberate Destruction 63
6.8.2 Personal Data in a Force's possession which was derived from another body 63
6.8.3 Hybrid FOI-Subject Access applications 64
6.8.4 'Accelerating' applications 64
6.9 Responding to applications 64
6.10 Enforced Subject Access 65
6.11 Criminal Procedure & Investigations Act 1996 (CPIA) 65
6.12 Updating Records from Subject Access applications 66
6.13 Formal withdrawal of Subject Access applications 66
6.14 Appeals/Complaints Process 66
6.15 Review and Retention of Subject Access Application Information by Police Forces 66
6.15.1 'National' (NIS) Applications 66
6.15.2 'Local' Applications 66
6.16 Standards 66

7 Other Rights and Complaints Resolution 70

7.1 Overview ... 70
7.2 Right to Prevent Processing Likely to Cause Damage or Distress (Section 10) ... 70
7.3 Right to Prevent Processing for the Purposes of Direct Marketing (Section 11) ... 72
7.4 Rights in Relation to Automated Decision Taking (Section 12) ... 72
7.5 Right to Compensation (Section 13) ... 73
7.6 Right to seek a Court Order for the Rectification, Blocking, Erasure or Destruction of Inaccurate personal data (Section 14) ... 73
7.7 Right to Request an Assessment by the Information Commissioner (Section 42) ... 74
7.8 Complaints Resolution ... 74
7.9 Standards ... 75

8 Security and other Protective Measures ... 76

8.1 Overview ... 76
8.2 The Seventh Principle: Introduction ... 76
8.3 ACPO National Vetting Policy for the Police Community ... 78
8.4 Data Processing Agreements ... 78
8.5 Development of, and Changes to, Information Systems ... 80
8.6 Data Protection/Information System Operating Rules ... 80
8.7 Relationship between Data Protection and Information Security Practitioners ... 81
8.8 Responsibilities and Structures ... 81
8.9 Standards ... 81

9 Transfers outside the European Economic Area ... 83

9.1 Overview ... 83
9.2 The Eighth Principle ... 83
9.2.1 Schedule 4 and Section 28 ... 83
9.2.2 Adequacy ... 84
9.2.3 Contractual Conditions ... 84
9.3 Police Force transfers outside the EEA ... 84

10 Handling Allegations of Criminal Offences under the Act ... 86

10.1 Overview ... 86
10.2 The Offences ... 86
10.2.1 Section 55 ... 87
10.2.2 Section 77 FOI Act ... 88
10.3 Process to be followed ... 88
10.3.1 Offence not connected to the Police ... 88
10.3.2 Offence or misconduct identified by, or reported to, the Police relating to Police-held personal data ... 89
10.3.3 Offence identified by, or reported to, the Information Commissioner relating to Police-held personal data. ... 90
10.4 The Role of the Information Commissioner's Head of Investigations ... 90
10.5 Related Offences ... 91
10.6 'Victim Care' ... 91
10.7 Standards ... 91

11 Disclosure of Personal Data by the Police ... 92

11.1 Overview ... 92
11.2 Introduction ... 92
11.3 Approach to disclosures of personal data ... 93
11.3.1 Define the personal data, the recipient, the purpose and the legal basis/power ... 93
11.3.2 Application of the data protection principles ... 93
11.3.3 Other considerations ... 94
11.4 Nationally approved Memoranda of Understanding and Policy ... 96
11.5 Personal Data Request Form (section 29) ... 96
11.6 Disclosures required by law or made in connection with legal proceedings etc. (section 35) ... 96

11.6.1 Section 35: Introduction 96
11.6.2 The non-disclosure provisions 97
11.6.3 Section 35(1): Disclosures required by law 97
11.6.4 Section 35(2): Disclosures made in connection with legal proceedings 99
11.7 'A to Z' Disclosure Reference 102
11.8 Standards 102

12 Powers of the Information Commissioner 104

12.1 Overview 104
12.2 The Criminal Justice and Immigration Act 2008 104

Appendix A: Standards 106

Appendix B: Exemptions 108

Appendix C: Template and Guidance for a Data Processing Agreement 111

Appendix D: Baseline Security requirements for Data Processing Agreements 121

Appendix E: Undertaking of Confidentiality 125

Appendix F: Personal Data Request Form 126

Appendix G: Data Protection/Information System Operating Rules Template 133

Appendix H: Version Control 138

Preface

The ACPO Data Protection Manual of Guidance (the manual) has been produced by the Association of Chief Police Officers (ACPO) to assist police forces in their statutory responsibility to comply with the Data Protection Act 1998 (the Act[1]).

The underlying philosophy of the manual is simple – data protection compliance is not merely a regulatory necessity, but is a core requirement to support effective policing. The manual identifies the structures, responsibilities, policies and processes that must be in place to ensure consistency in the way the Act is applied throughout the police service. This is supported by baseline standards that can be found throughout the document.

The primary target audience for the manual are data protection officers, information system owners, and chief officers (in their capacity as 'data controllers' under the Act). However, it has also been designed to be accessible by all police officers and police staff. This guidance is not intended to be a detailed analysis of every aspect of the Act (that function is adequately served by reference books and guidance offered by the Information Commissioner and the Department of Constitutional Affairs).

The manual should therefore be regarded as a document that helps create an environment across the police service in which compliance can be achieved and as a means of providing guidance in areas of police business where the Act is regularly applied.

The manual primarily focuses on the use by the police of personal data for operational purposes. However, it also recognises that the police service also processes personal data for supporting functions such as the administration of staff. Readers are therefore encouraged to be aware of the Information Commissioner's guidance contained in his Employment Practices Code.

The manual consists of two parts:

- Part 1: Standards (this document);
- Part 2: Audit (a 'sister' document that provides detailed guidance on data protection compliance auditing).

In terms of the recent changes to the Act, the manual takes into account the amendments made by the enactment of the Freedom of Information Act 2000. These include:

- the creation of a new category of personal data for the police (as a 'public authority');
- the modification of the standard notification to the Information Commissioner;
- the introduction of a cost exemption to the new category of personal data, and;
- the creation of an offence to alter, deface, block, erase, destroy or conceal personal data sought under subject access[2].

Similarly, the manual also takes into account the Statutory Code of Practice on the Management of Police Information 2005 (MoPI Statutory CoP) and the Guidance on Management of Police Information 2006 ('MoPI Guidance')[3].

Ian Readhead QPM LLB
ACPO Data Protection, Freedom of Information and Records Management Portfolio Holder

---

[1] The Act has been followed by a number of related statutory instruments and the Freedom of Information Act 2000 – the Department of Constitutional Affairs has introduced a useful website 'The UK Statute Law Database' where these can be found.
[2] For further information on the Freedom of Information Act see the ACPO Manual of Guidance Freedom of Information.
[3] The 'MoPI Guidance' does not have the scope or necessary level of detail to provide sufficient data protection guidance in all areas; hence the need for this manual and supporting force policy, procedures and guidance.

1 Responsibilities and Structures

1.1 Overview

Each chief officer (as 'data controller') has a legal obligation to ensure that all processing of personal data, by or on behalf of their police force is in accordance with the Act[4]. Therefore, chief officers must establish certain measures to help ensure compliance with the law.

Chapter 1 describes these measures in detail. They include:

- the allocation of specific compliance responsibilities to certain staff;
- the establishment of effective reporting lines;
- the implementation of data protection awareness training for all staff;
- the publication of data protection guidance for all staff outlining the key elements of the Act; and;
- the undertaking of data protection compliance auditing, data quality auditing and monitoring.

At a national level chief officers support the activities of an ACPO Data Protection Portfolio (currently combined with the ACPO Freedom of Information Portfolio) reporting to the ACPO Information Management Business Area.

1.2 Responsibilities

1.2.1 Chief Officer – Data Controller

The chief officer is legally responsible for their force's compliance with the Data Protection Act.

The chief officer cannot delegate this legal responsibility.

Where a police force is involved in partnership working in which both the police force and the partner(s) determine the purpose and manner in which personal data is processed, then the police force and its partner(s) will both be responsible as 'data controllers' - either 'jointly' or 'in common'.

'Jointly' applies to situations where both the purpose and the manner of the processing is determined by different data controllers acting together. The Information Commissioner has advised that this 'may well cover matters such as joint actions involving two or more forces'.

'In common' applies where the data controllers share a pool of personal data, each processing it independently of one another. The Information Commissioner has advised that this 'would appear to reflect how the Police National Computer works at a very general level'.

In order for a police force to achieve compliance with the Act it is implicit to establish an effective reporting line in place between the chief officer and the force data protection officer (see 1.2.4 xii and 1.3).

1.2.2 Senior Manager

The chief officer must formally designate an officer of ACPO rank or police staff equivalent to both support and oversee the management of data protection matters, ensuring that relevant police force

[4] See Data Protection Act (DPA) section 1 for definitions of 'personal data', 'processing', 'data processor', 'data controller'; DPA section 4 for obligation to comply with principles, and DPA schedule 1 for the 'data protection principles'.

policies, procedures and guidelines reflect the requirements of this manual.[5]

1.2.3 Senior Information Risk Owner (SIRO)

The senior manager described in 1.2.2 may also perform the function of Senior Information Risk Owner (SIRO) as defined by INFOSEC Standard 2 and required by the ACPO Community Security Police (CSP).

Although the SIRO is closely associated with a police force's information security work, the role is also significant in achieving compliance with the Act, in particular the requirements of the seventh principle.

By designating a SIRO, a police force demonstrates that there is a mechanism and decision-making process in place, at senior level, that considers appropriate technical and/or organisational measures for the type of information (including personal data), together with any risks to information and the business.

The SIRO is required to understand how the strategic business goals of the police force may be impacted upon by information system failures. The SIRO also ensures that management of information risks are weighed alongside the management of other risks facing the organisations such as financial, legal and operational risks. This role is supported by the information assurance resources, including accreditors and information security officers. However the ownership of the risk remains with the SIRO.

1.2.4 Data Protection Officer

A force data protection officer[6] will be appointed, or formally nominated, to manage the chief officer's statutory obligations in respect of the Act. The data protection officer's documented responsibilities *may* include[7]:

i) managing the chief officer's statutory obligations in respect of the Act including; notification of processing to the Information Commissioner; compliance with the data protection principles and securing individuals rights under the Act, including subject access requests;

ii) maintaining an up to date knowledge of, and advising on relevant legislation and general developments in data protection and related matters;

iii) promoting awareness of data protection matters through training, policy development, advice and guidance;

iv) undertaking systematic auditing and monitoring of information and systems in accordance with the forthcoming companion to this document, ACPO Data Protection Manual of Guidance Part 2: Audit;

v) ensuring information and systems comply with the relevant legislation including the Act;

vi) ensuring that appropriate security arrangements exist to protect information, including where necessary that suitable contracts are drawn up relating to the processing of police information by

---

[5] 2.5 of MoPI Guidance describes the requirement for an Information Management Strategy (IMS) for each police force. A template IMS has been produced by Centrex entitled 'Information Management Strategy, Standards and Working Practices'. Section 6.4 of that document introduces the term 'Chief Information Officer or equivalent' whose remit encompasses this role of 'senior manager' in this manual.

[6] This manual uses the term 'data protection officer' to refer to those individuals within forces who manage their chief officer's responsibilities towards the Act. It is recognised that within some forces those activities may be designated to more than one person and to persons not formally known as the 'data protection officer'.

[7] 2.5 of MoPI Guidance describes the requirement for an Information Management Strategy (IMS) for each police force. A template IMS has been produced by Centrex entitled 'Information Management Strategy, Standards and Working Practices'. Section 6.7.4 of that document describes a data protection officer's responsibilities which have been copied verbatim here. It is acknowledged that the role of data protection officers across police forces are likely to vary according to local structures and requirements.

third parties;

vii) investigating and resolving complaints made in relation to the handling of personal information (in relation to data protection);

viii) assisting where appropriate in the investigation of disciplinary and criminal matters relating to data protection;

ix) liaising on all data protection matters between the force and relevant regional or national bodies (including the ACPO Data Protection and Freedom of Information Portfolio Group and the Information Commissioner);

x) liaising with BCU Commanders/Department Heads when necessary to provide guidance and support on data protection matters;

xi) ensuring that the Data Protection Manual of Guidance is disseminated and adhered to forcewide;

xii) liaising directly with the chief officer;

xii) liaising regularly with the force Information Security Officer or equivalent.

Factors such as the size of the police force, the amount of resources devoted to data protection matters and local structures may result in variations in the scope and volume of work undertaken by data protection officers. If, as a consequence of such factors, a data protection officer is not in a position to undertake any of the listed responsibilities then the police force will document who will do so.

1.2.5 Senior Responsible Officer (SRO), Senior System Owner (SSO) and Information System Owner

These various titles are given to those staff responsible for information systems, through the life cycle of those systems - from project stage, through live environment and to the systems' decommissioning. Those staff play a significant role in helping to ensure information security, and, where personal data is processed, to achieve compliance with the Act.

A person should be assigned with ensuring that a programme or project meets its objectives as agreed with the SIRO and board level business owners. The role includes understanding the risk to the programme or project and its information, taking account of legal (including the Act), business and operational requirements. It also includes responsibility for data quality and for documented operating procedures (see data protection/information systems operating rules at 8.6).

As a minimum, police forces will ensure that these responsibilities are assigned for information systems processing the most sensitive and operationally impactive, personal data; for example, crime recording/management, intelligence, PNC, prosecutions, human resources, incident recording and management, and other systems 'feeding' the in Impact Nominal Index (INI).

Further detail on equivalent roles and responsibilities of information system owners are contained in two recent documents that support the MoPI Guidance: Page 41 of the MoPI Threshold Standards contains a summary of the roles, responsibilities and competencies of 'system owners'. In addition, section 2.5 of the MoPI Guidance describes the requirement for an Information Management Strategy (IMS) for each police force. A template IMS has been produced by Centrex entitled 'Information Management Strategy, Standards and Working Practices'. Section 6.6 of that document describes the functions and responsibilities of business process/systems owners.

1.2.6 All Staff

Every police officer, member of police staff, police community support officer, special constable, volunteer, data processor, contractor and approved persons working for or on behalf of the police (also see 8.4) having access to personal data is required to comply with the requirements of the Act and any

supporting local policy or procedure designed to help achieve compliance.

1.3 Structure

Each police force must have in place a management structure that will allow an effective dialogue on data protection issues between chief officers, the data protection officer and other staff.

Police forces must also ensure that structures and procedures are established to ensure that any concerns regarding data protection compliance within a police force are directed to the data protection officer in a timely manner. See chapter 10 for instances where those concerns relate to allegations of criminal offences under the Act.

1.4 Data Protection Training and Awareness

In a judgement in the summer of 2005 the Information Tribunal stated:

> "The Tribunal also respectfully suggests that officers and staff at all levels be formally acquainted with a better understanding of all pertinent data protection requirements."

Police forces will develop and implement training strategies that incorporate data protection aspects[8], and are designed to ensure that all police officers, police staff, volunteers and others involved in the processing of personal data are aware of the requirements that the Act places upon them.

Training strategies must be designed to ensure that all staff receive, as a minimum, baseline awareness training, with further specialist training supplied as required dependant on role and circumstances.

Police forces must ensure that records are maintained for all staff receiving training. The records should evidence what training has been provided to whom and when in order to enable subsequent analysis by the data protection officer and other staff as required. Such records are likely to assist as evidence in misuse enquiries and help police forces meet their obligations under the seventh principle of the Act.

1.5 Publication of Data Protection Guidance

Police forces will provide their staff involved in the processing of personal data with guidance designed to make them aware of the requirements the Act places upon them. The guidance may take the form of a high-level force policy explaining the key elements of the Act such as the principles, exemptions and offences, plus more specific guidance to cover particular areas of interest, such as the handling of subject access applications, disclosure, and data processing agreements.

Data protection officers will also make arrangements with those developing policy to ensure that where necessary, data protection requirements are considered.

Other guidance may also be produced for the benefit of external audiences. For example, advice to the public as how to exercise their subject access rights.

1.6 Data Protection Compliance Auditing, Data Quality Auditing and Monitoring

In order to help achieve compliance with the Act police forces will be expected to undertake data protection compliance audits, inspections and monitoring in accordance with the companion to this document, ACPO Data Protection Manual of Guidance Part 2: Audit.

The Information Commissioner has produced a Data Protection Audit Manual, which looks at compliance with the Act as a whole, rather than just concentrating on data quality issues. Police forces are therefore encouraged to adopt relevant practices from the Information Commissioner's Audit Manual.

---

[8] The DPA seventh principle and DPA section 4(4) effectively require data protection awareness training for all persons involved in the processing of personal data.

1.7 ACPO Data Protection Portfolio

1.7.1 Appointment of Portfolio Holder

ACPO's Information Management Business Area (IMBA) will invite an officer of ACPO rank to maintain a Data Protection Portfolio (currently combined with a Freedom of Information Portfolio). There will be no prescribed time limit for this position. The role's primary aim will be to ensure a consistently high level of compliance with the Act throughout the Police Service.

1.7.2 Portfolio Group Terms of Reference and Structure

The terms of reference and structure for the portfolio will be determined by the ACPO ranked officer maintaining the portfolio.

1.8 Standards

Standard	Source
ACPO/Senior Manager lead on data protection matters identified within the police force	1.2.2
Data protection officer appointed or nominated within the police force and responsibilities documented	1.2.4
Information system owners formally identified for key systems within the police force and tasked	1.2.5
Effective reporting lines established within the police force	1.3
Data protection training provided for all staff within the police force	1.4
Data protection guidance published within the police force	1.5
Data protection auditing and monitoring carried out in accordance with the ACPO Data Protection Manual of Guidance Part 2: Audit	1.6

2 The Police, Processing and Principles

2.1 Overview

This chapter provides a brief introduction to the data protection principles and the processing of personal data by the police. Subsequent chapters examine the principles in greater depth.

2.2 Compliance with the principles

The data protection principles[9] set out the basic standards governing the 'processing' of personal data[10].

All chief officers, in their capacity as 'data controllers', must comply with the principles unless an exemption applies[11].

The principles are as follows:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:-

(a) at least one of the conditions in Schedule 2 is met, and

(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Failure to comply with the principles exposes police forces to the risk of enforcement or legal action from the Information Commissioner[12] and/or 'data subjects'[13]. Such failures may also lead to a decline in operational effectiveness and adverse publicity.

---

[9] The principles can be found within DPA schedule 1 part I and part II, with the requirement to comply with them within DPA section 4.

[10] 'Processing and 'personal data' are defined within DPA section 1.

[11] A summary of the exemptions under the Act can be found in appendix b.

[12] The enforcement regime is detailed in DPA Part V.

[13] 'Data subject' is defined within DPA section 1(1).

Schedule 1 part 2 contains further interpretive provisions for most of the principles and will be considered in addition to the principles themselves.

2.3 Processing of personal data by the police

'Processing' has a very broad meaning, encompassing 'obtaining, recording or holding' the personal data and carrying out various operations in respect of it including organising, adapting, altering, retrieving, consulting, using, disclosing, aligning, combining, erasing or blocking - it is difficult to think of any activity relating to personal data that would not fall under the definition of 'processing'.

The police process, through a wide variety of means, a vast and diverse volume of personal data relating to staff, victims, witnesses, offenders, suspects, and others. The following record types (not an exclusive list), routinely held electronically by the police, will tend to contain personal data:

Statement
Likely to contain personal data of the person providing statement; and on occasions that of other people whose behaviour/activity is described in the statement;

Custody Record
Likely to contain personal data of the subject of the custody record and others whose behaviour/activity is described within it;

Crime Report
Likely to contain personal data of the person reporting the crime, witnesses, suspects and others whose behaviour/activity is described within it.

Incident Log
Likely to contain personal data of the person reporting the incident, witnesses, suspects and others whose behaviour/activity is described in the incident log;

Intelligence Report
Likely to contain personal data of the source and persons mentioned in the intelligence report;

Personnel File
Likely to contain personal data of the person subject of personnel file, and their associated family/household members;

Nominal Record
Likely to contain personal data of the subject of the nominal record, associated individuals mentioned e.g. known associates, family members.

The mention of an officer's name or other identifiers, where he or she is acting in an overt professional capacity, *on its own* is unlikely to represent their personal data.

However, a vehicle registration mark (VRM) processed by the police will be regarded as personal data on the basis that police forces have the capacity to identify vehicle keepers from that information.

Any police-held information which is deemed not to be 'personal data' may be accessible to the public under the Freedom of Information Act 2000 (FOI Act). In limited circumstances third-party personal data may also be accessible via requests made under the FOI Act.

2.4 The use of de-personalised information

In some instances it may be possible for a police force to achieve a particular purpose(s) using information that is not personal data. Such information will consequently fall outside the scope of the Act[14], and may be created by 'anonymising' or 'de-personalising' personal data. However, care must be

[14] However, this does not negate any responsibility under the ACPO Community Security Policy.

taken if using this approach to ensure that any recipient of the de-personalised information does not have the ability to 're-create' the personal data using other information they are likely to have access to.

3 Fair and Lawful Processing

3.1 Overview

This chapter examines the first and second principles and their application within the police context.

It starts by introducing the first principle, then goes on to describe the concepts of lawful and fair processing, and the requirements to comply with the schedule 2 ('legitimate processing') and schedule 3 ('sensitive personal data') conditions.

The chapter also covers the second principle requirements of notification and compatible use of personal data.

A checklist is provided towards the end of the chapter and is designed to assist navigation through the fair and lawful elements of the first and second principles.

3.2 The First Principle

3.2.1 First Principle: Introduction

The first principle tends to be the most significant of the eight principles. It includes detailed conditions that apply to the obtaining and processing of personal data; and a requirement for lawfulness which necessitates consideration of other legal rules.

The first principle requires that personal data shall be processed lawfully and fairly and in particular should not be processed unless at least one of the conditions in schedule 2 is met, and, in the case of 'sensitive personal data'[15], at least one of the conditions in schedule 3 is also met.

In short it requires the police force to ensure that it has a legitimate basis for the processing of all personal data. Therefore if a police force cannot comply with this principle the processing will be in breach of the Act.

'Lawfully' and 'fairly' are not precisely defined within the Act, though part 2 of schedule 1 provides interpretation of 'fairly' in terms of obtaining.

The exemption at section 29(1) provides the police with a useful relief from some requirements of the first principle where it is necessary to prevent or detect crime, or to apprehend or prosecute offenders.

3.2.2 First Principle: Lawful Processing

Personal data must not be processed in contravention of any statute, legal obligation or restriction – to do so would represent unlawful[16] processing and thus breach the first principle. There should be a positive legal justification for the processing.

The power for the police to process personal data can be derived from a number of sources. For example, the police have a duty to meet the 'policing purpose' as defined in section 2.2.2.2 of the MoPI Statutory CoP as:

- Protecting life and property;
- Preserving order;
- Preventing the commissioning of offences;

[15] 'Sensitive personal data' is defined within DPA section 2.

[16] 'Unlawful' has been defined as 'something which is contrary to some law or enactment or is done without lawful justification or excuse' – RvR [1994] 4 All E.R. 481. Irrespective of the Act, any activity by the police must be lawful. The terms 'lawful' and 'unlawful' apply equally to criminal and civil law.

- Bringing offenders to justice, and;
- Any duty or responsibility of the police arising from common or statute law.

The police may also be subject to other statutory obligations which require or permit certain types of processing, such as those under the Police Act 1996, or requirements to provide information to the Child Support Agency and other 'Governmental' bodies, or to process employment-related personal data.

In addition, the police may be obliged to process personal data through the order of a court.

Generally where the police process personal data for the 'policing purpose' it is unlikely that they will fall foul of this particular element of the first principle. However, the police must ensure that access to personal data is restricted to a 'need-to-know' basis. In the absence of such a need access is unlikely to represent lawful processing.

Unlawful processing may arise where the police process personal data:

beyond or in contravention of their statutory or common law powers (i.e. ultra vires), for example:

The police sell the names and addresses of burglary victims to companies trying to sell double-glazing;

or,

in breach of an obligation of confidentiality (see 3.2.2.1), for example:

The police publish the names and home addresses of all staff on the internet;

or,

in breach of any law or prohibitions, for example:

The police obtain personal data in contravention of the Regulation of Investigatory Powers Act 2000;

The police process personal data in contravention of the Data Protection Act 1998 itself;

The police process personal data in a manner which breaches the Article 8 rights of the Human Rights Act 1998;

or,

in breach of an enforceable contractual agreement.

3.2.2.1 Lawful Processing: Confidentiality

There are circumstances where an obligation of confidence arises between the police and a data subject and to breach that confidence without reasonable justification would be likely to represent unlawful processing.

The obligation of confidence means that the police are restricted from processing the personal data for a purpose other than that for which it was provided unless:

The data subject consented to the processing; or,

The processing was required by law; or,

The processing was in the public interest.

The nature of the 'policing purpose' is that either of the latter two grounds are likely to apply where the

obligation of confidence needs to be breached to prevent or detect crime, apprehend or prosecute offenders.

The Information Commissioner has produced useful guidance on confidentiality as part of a series of a library of good practice guidance designed to aid the understanding and application of the Freedom of Information Act 2000.

3.2.3 First Principle: Fair Processing

Subject to exemptions[17], personal data must be obtained and further processed 'fairly'.

Put simply, any data subject should not be 'surprised' by the police's use of their personal data. However, the potential for such surprise will be affected by the data subject's legitimate expectations.

Therefore it is likely that those working for the police would find it reasonable and unsurprising for the police as their employer to use their personal data for staff administration, payroll, training, and supervision purposes. The selling of their personal data to other bodies would be considered unexpected and unreasonable. It is also likely that members of the public who contact the police would expect that if they reported or witnessed a crime or incident the police would collect their personal data and further process it for those purposes. However, it would be unreasonable to expect their personal data to be provided automatically in all cases to the media. Similarly, those subject to police investigations will have a legitimate expectation that the police will process their personal data for the 'policing purpose'.

The Act assists with the interpretation of the fairness requirement of the principle in schedule 1 part 2 paragraphs 1 to 3[18] - termed the 'fair processing requirements' by the Information Commissioner – which are summarised in the remainder of 3.2.3 and its sub sections.

Compliance with the fair processing requirements will not in itself necessarily ensure fair processing.

3.2.3.1 Fair Processing Requirements[19]: Obtaining

Paragraph 1 establishes that in determining whether personal data is processed fairly consideration has to be given to the method it was obtained - including whether any person from whom the personal data was obtained was deceived or misled as to the purpose of processing. Within the policing context this provision may be breached in the following example:

> *Police staff were asked to have their photographs taken in order that they could be used specifically for police staff identity cards. However, the photographs were subsequently published on the police force internet for an incompatible purpose.*

The second part of paragraph 1 provides that personal data is considered to have been 'fairly obtained' if it is from a person who is authorised by law to supply it or is required to supply it by, or under any enactment. One example of this within the policing context would be:

> *The requirement under statute for the police to provide details of staff salaries to the Inland Revenue.*

This provision is subject to paragraph 2, which sets out the information which must be provided to data subjects (see 3.2.3.2).

3.2.3.2 Fair Processing Requirements[20]: 'Fair Processing Notices'

Paragraph 2 provides that personal data is not to be treated as processed fairly unless certain

---

[17] In the policing context the most relevant exemption is to be found at DPA section 29(1)
[18] DPA Schedule 1 part 2 paragraph 4 has yet to be enabled.
[19] 'Fair Processing Requirements' are DPA schedule 1 part 2 paragraphs 1 to 4
[20] 'Fair Processing Requirements' are DPA schedule 1 part 2 paragraphs 1 to 4

information is provided to a data subject. This can be at the time the personal data is gathered from them or, if it is obtained by another route, either before the 'relevant time'[21] or as soon as practicable thereafter. 3.2.3.3 describes exemptions to this requirement.

That certain information, known as 'the specified information' or 'fair processing information' is often provided to data subjects in the form of a written or verbal 'fair processing notice'.

In many cases police officers and police staff will unwittingly provide such a 'fair processing notice' by telling those that come into contact with the police what they intend to do as a result of that contact.

The 'specified information' or 'fair processing information' consists of the following:

(a) the identity of the data controller,

(b) if the data controller has nominated a representative for the purposes of the Act, the identity of that representative,

(c) the purpose or purposes for which the data are intended to be processed, and

(d) any further information which is necessary, taking into account the specific circumstances in which the data are or are to be processed, to enable processing in respect of the data subject to be fair.

This will be provided to data subjects or be made readily available to them, so far as practicable, via a 'fair processing notice' when personal data is obtained by the police.

The Information Commissioner's legal guidance advises that in deciding whether and, if so, what further information is 'necessary' to satisfy (d) above the police:

'Should consider what processing of personal data they will be carrying out once the data have been obtained and consider whether or not data subjects are likely to understand the following:-

(a) the purposes for which their personal data are going to be processed;

(b) the likely consequences of such processing such that the data subject is able to make a judgement as to the nature and extent of the processing; and

(c) whether particular disclosures can reasonably be envisaged.

It would be expected that the more unforeseen the consequences of processing the more likely it is that the data controller will be expected to provide further information.'

Examples of 'any other information necessary to make the processing fair' may include the provision of:

retention/review periods;

likely disclosures;

likely overseas transfers;

details as to how the data subject can enforce their rights under the Act.

---

[21] The 'relevant time' is defined under DPA schedule 1 part 2 paragraph 2(2) – where the police intend to 'keep the personal data to themselves' this will be when processing first takes place; where the personal data is disclosed by the police this will be at that time; where the police decide not to disclose personal data originally intended for disclosure this will be at the time of that decision.

3.2.3.3 Fair Processing Requirements[22]: Exemptions from providing 'Fair Processing Notices'

Where the personal data is obtained other than from the data subject there are two key exemptions [23] from the requirement to provide a 'fair processing notice'. However, the ability to rely on either exception does not absolve the police from the overriding duty to process personal data fairly, and, in any case, a 'fair processing notice' must still be supplied to any individual who requests one.

The exemptions referred to above occur where the provision of a 'fair processing notice' would involve a 'disproportionate effort'[24] or where it is necessary for the police to record the information to be contained in the data, or to disclose the data, to comply with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.

The Secretary of State has prescribed further conditions, by way of 'appropriate safeguards', which must also be met for the exception to be available. These are contained in the Data Protection (Conditions Under Paragraph 3 of Part II of Schedule I) Order 2000 (S.I. No 185).

Where the police rely upon the disproportionate effort condition above, the police force may keep a record of the reasons why it believes the disapplication of the 'fair processing notice' is necessary. When determining the 'disproportionate effort' the police will consider factors such as the nature of the data, the length of time and the cost in providing the information, balanced against any prejudicial effect to the data subject.

3.2.3.4 The Police's use of 'Fair Processing Notices'

The police will obtain and further process personal data relating to a wide variety of data subjects, including staff, victims, and criminals, and any application of the fairness requirement, including the use of 'fair processing notices' will need to be adjusted according to the nature of that relationship.

A pragmatic and flexible attitude will be adopted by police forces including a 'layered' approach, with an initial high level 'fair processing notice' 'up front' to the public with advice as to where other more detailed information can be obtained from.

Police forces will also ensure that an open relationship is maintained with their own staff through the use of 'fair processing notices' as widely as possible as part of the employer-employee relationship. This should not be merely for compliance with the Act, but as part of a wider respect for employees.

The police are encouraged to ensure that general 'fair processing notices' are provided in the circumstances outlined below. In addition the police will ensure that ad hoc 'fair processing notices' are provided as and when required:

On a general 'fair processing notice' to be made publicly available as a leaflet describing in broad terms how the police process handle personal data.

On a general 'fair processing notice' to be made publicly available on police force internet sites;

On the footers of internal and external email;

On all police force forms and associated policy related to employment or personnel matters – including recruitment, commendations, discipline, personal development plans, payroll, sickness, and contracts;

On signs for overt CCTV systems operated by the police force (as per the Information Commissioner's CCTV Guidance);

---

[22] 'Fair processing requirements' are DPA schedule 1 part 2 paragraphs 1 to 4
[23] Provided at DPA schedule 1 Part 2 Paragraph 3.
[24] 'Disproportionate effort' is not defined in the Act.

On signs for overt Automated Number Place Recognition (ANPR) systems;

To victims of crime in respect of referrals to Victim Support (as per ACPO – Victim Support Victim Referral Agreement, based on Home Office Circular 44/2001).

As well as the exemption described in 3.2.3.3 above section 29(1) of the Act provides relief from the fairness requirements of the first principle to the extent necessary to prevent prejudice to the prevention or detection of crime, or the apprehension or prosecution of offenders.

Within the policing context the exemption means that in many operational scenarios the police are unlikely to be required to be 'fair' towards data subjects; for example:

Section 29(1) would apply where a data subject's personal data was being processed through him/her being the subject of a confidential criminal investigation and any disclosure of that fact would be likely to prejudice the investigation or other investigations.

Police forces are not expected to place 'fair processing notices' on telephone lines that may receive emergency calls (including misdirected ones) because of the associated risk of harm that may be caused through the delay in response to the call.

Various other exemptions from the fairness element of the first principle can be found in appendix b - they include national security (section 28) and legal proceedings (section 35).

A generic fair processing notice has been placed on the Essex Police website. Forces may wish to adopt or adapt it for their own purposes.

3.2.4 First Principle: Schedule 2 ('Legitimate Processing') Conditions

3.2.4.1 Schedule 2: Introduction

The first principle requires that as well as the lawfulness and fairness requirements, personal data shall not be processed unless at least one of the conditions in schedule 2 is met. If 'sensitive personal data'[25] is to be processed then a schedule 3 condition must also be satisfied (see 3.2.5).

The conditions recognise that the processing of any personal data is an invasion of the data subject's information privacy, and consequently the conditions are designed to create a threshold to prevent any unjustified processing.

There is no explicit requirement on the police to document the condition(s) upon which processing is legitimised, but experience has shown that in dispute cases the Information Commissioner will seek an early confirmation of the conditions selected. It may be prudent for the police to identify as many schedule 2 (and, where necessary, schedule 3) conditions as possible for processing for a particular purpose.

Achieving a schedule 2 (and, where necessary, schedule 3) condition will not, on its own, guarantee that processing is fair and lawful. The general requirement that data be processed fairly and lawfully must be satisfied in addition to meeting the conditions.

There are only a very limited number of exemptions from the schedule 2 and 3 conditions, including those for national security (section 28) and domestic purposes (section 36) – both exemptions also provide relief from other elements of the Act (see appendix b).

The schedule 2 conditions and constituent grounds likely to be most relevant to the police are as follows[26]:

[25] Sensitive personal data is defined in DPA section 2.

[26] Of course the police may use any of the other conditions where appropriate.

1. The data subject has given his consent to the processing. ('Consent')

3. The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract. ('Non Contractual Legal Obligations')

4. The processing is necessary in order to protect the vital interests of the data subject. ('Vital Interests')

5. The processing is necessary:-
(a) the administration of justice;
(b) for the exercise of any functions conferred by or under any enactment;
(c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department;
(d) for the exercise of any other functions of a public nature exercised in the public interest. ('Public Functions')

6(1) The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject. ('Legitimate Interests')

In particular cases other schedule 2 grounds, not described above, may also be applicable.

The majority of the schedule 2 (and 3) conditions stipulate that the processing must be 'necessary' for the purpose set out in that particular condition. The Information Commissioner has provided the following guidance on 'necessity' in his legal guidance:

"Data controllers will need to consider objectively whether the purposes for which the data are being processed are valid; such purposes can only be achieved by the processing of personal data, and, the processing is proportionate to the aim pursued."

Where the police rely on any of the schedule 2 conditions under paragraphs 1 to 4 the data subject is unable to claim their right to object to processing under section 10 of the Act (see 7.2).

The schedule 2 conditions likely to be of most relevance to the police are examined in more detail in the following subsections 3.2.4.2 to 3.2.4.6.

3.2.4.2 Schedule 2: 'Consent'

The first schedule 2 condition requires that the data subject has given his/her consent to the processing.

ACPO's view is that as no one condition carries more weight than any other, and consent is not particularly easy to achieve and may be withdrawn at any time, the police will attempt to legitimise processing using other conditions and only revert to consent in the absence of another condition.

In his legal guidance the Information Commissioner has provided the following guidance on 'consent':

"Consent is not defined in the Act. The existence or validity of consent will need to be assessed in the light of the facts. To assist in understanding what may or may not amount to consent in any particular case it is helpful to refer back to the Directive. This defines "the data subject's consent" as:-

..any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

The fact that the data subject must "signify" his agreement means that there must be some active communication between the parties. A data subject may "signify" agreement other than in writing. Data controllers cannot infer consent from non-response to a communication, for example from a

customer's failure to return or respond to a leaflet.

The adequacy of any consent or purported consent must be evaluated. For example, consent obtained under duress or on the basis of misleading information will not be a valid basis for processing.

Where a data subject does not signify his agreement to personal data relating to him being processed, but is given an opportunity to object to such processing, although this does not amount to consent for the purposes of the Act, it may provide the data controller with the basis to rely upon another Schedule 2 condition, for example, the legitimate interests condition, provided that the data subject is given the right to object before the data are obtained.

Consent must be appropriate to the particular circumstances. For example, if the processing is intended to continue after the end of a trading relationship then the consent should cover those circumstances. However, it must be recognised that even when consent has been given it will not necessarily endure forever. While in most cases consent will endure for as long as the processing to which it relates continues, data controllers should recognise that, depending upon the nature of the consent given and the circumstances of the processing, the individual may be able to withdraw consent."

3.2.4.3 Schedule 2: 'Non Contractual Legal Obligations'

The third schedule 2 condition requires that the processing is necessary for compliance with any legal obligation to which the police force is subject, other than an obligation imposed by a contract.

This condition deals with the situation where the police are obliged by law to process personal data, as opposed to enforceable agreement with the data subject which necessitates the processing of personal data.

Likely examples of use within the police context include:

Disclosure of an employee's personal data by the police to Government Agencies/Departments required under statute;

Disclosure by the police of personal data to a court in response to a court order.

3.2.4.4 Schedule 2: 'Vital Interests'

The fourth schedule 2 condition requires that the processing is necessary in order to protect the vital interests of the data subject.

The Information Commissioner's legal guidance advises:

"The Commissioner considers that reliance on this condition may only be claimed where the processing is necessary for matters of life and death, for example, the disclosure of a data subject's medical history to a hospital casualty department treating the data subject after a serious road accident".

However, the police are likely to use a less restrictive interpretation than 'matters of life and death', and consequently may rely on this condition for example, where processing of personal data is required in order to prevent harm to an individual:

Disclosure by the police of personal data relating to a missing person to the media.

3.2.4.5 Schedule 2: 'Public Functions'

The fifth schedule 2 condition allows the processing of personal data where it is necessary for (a) the administration of justice; (b) for the exercise of any functions conferred by or under any enactment; (c)

for the exercise of any functions of the Crown, a Minister of the Crown or a government department; (d) for the exercise of any other functions of a public nature exercised in the public interest.

The Act does not define 'administration of justice', but it does seem to encompass much police activity such as crime prevention or detection and the apprehension and prosecution of offenders, and the supporting activities that enable them.

These grounds cover much of the processing of personal data by the police. For example:

> *Processing by the police of personal data relating to employees, victims, witnesses, suspects and offenders for the purposes of prevention or detection of crime, apprehension or prosecution of offenders;*
>
> *Processing of personal data by the police necessary to maintain an effective and efficient police force as required by sections 6, 8, 10(2) the Police Act 1996.*

3.2.4.6 Schedule 2: 'Legitimate Interests'

The sixth schedule 2 condition requires that the processing is necessary for the purposes of legitimate interests pursued by the police or by the third party or parties to whom the data is disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

This condition requires a 'balancing act', assessing both the legitimate interests of the data subject and the police (or third party to whom the personal data is disclosed), and an appraisal of which should take priority.

The Information Commissioner's legal guidance states:

> 'The Commissioner takes a wide view of the legitimate interests condition and recommends that two tests be applied to establish whether this condition may be appropriate in any particular case. The first is the establishment of the legitimacy of the interests pursued by the data controller or the third party to whom the data are to be disclosed and the second is whether the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject whose interests override those of the data controller. The fact that the processing of the personal data may prejudice a particular data subject does not necessarily render the whole processing operation prejudicial to all the data subjects'.

It is not possible to provide a generic balancing act that can be used by the police in all circumstances when assessing this appropriateness of the use of this condition. However, it may be useful for police forces to identify and quantify the likely harm to the data subject, other individuals, the wider public and the police should a particular course of action be followed. Such an assessment could include contacting the data subject to seek their views on any likely impact[27], or examining the effects of similar processing operations in the past.

3.2.5 First Principle: Schedule 3 (Sensitive Personal Data) Conditions

3.2.5.1 Schedule 3: Introduction

The first principle requires that, as well as the lawfulness and fairness requirements, personal data shall not be processed unless at least one of the conditions in schedule 2 is met (see 3.2.4[28]) and where 'sensitive personal data' is being processed too, then a schedule 3 condition must also be satisfied.

Section 2 of the Act defines categories of 'sensitive personal data', namely, personal data consisting of information as to:-

---

[27] The fairness requirements elsewhere in the first principle may require such contact anyway.

[28] Readers are encouraged to read 3.2.4 prior to reading 3.2.5 as some of the concepts covered in the former are relevant to the latter.

(a) the racial or ethnic origin of the data subject;
(b) his political opinions;
(c) his religious beliefs or other beliefs of a similar nature;
(d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992);
(e) his physical or mental health or condition;
(f) his sexual life;
(g) the commission or alleged commission by him of any offence; or
(h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

The police are likely to process a significant amount of sensitive personal data in most of the categories above. Likely data subjects include suspects and offenders, as well as witnesses, victims, members of staff and others. Whoever they are, their sensitive personal data cannot be processed unless one or more schedule 3 conditions is met.

The schedule 3 conditions and constituent grounds likely to be most relevant to the police are detailed below[29]. They are more restrictive than the schedule 2 conditions:

1. The data subject has given his explicit consent to the processing of the personal data. ('Explicit Consent')

3. The processing is necessary:-
(a) in order to protect the vital interests of the data subject or another person, in a case where:-
(i) consent cannot be given by or on behalf of the data subject, or
(ii) the data controller cannot reasonably be expected to obtain the consent of the data subject, or
(b) in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld. ('Vital Interests')

6. The processing:-
(a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),
(b) is necessary for the purpose of obtaining legal advice, or
(c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights. ('Legal Proceedings')

7(1) The processing is necessary:-
(a) for the administration of justice,
(b) for the exercise of any functions conferred on any person (including a constable) by or under an enactment, or
(c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department. ('Public Functions')

When the Act was introduced it included a provision at paragraph 10 of Schedule 3 that allowed the Secretary of State to define additional circumstances that would permit the processing of Sensitive personal data. The Secretary of State made use of that provision with Statutory Instrument 2000 No. 417 The Data Protection (Processing of Sensitive Personal Data) Order 2000. Included amongst its ten new provisions are two of particular relevance to the Police:

Paragraph 1 which covers certain processing for the purposes of the prevention or detection of any unlawful act, where seeking the consent of the data subject to the processing would prejudice those purposes - "1. (1)The processing - (a) is in the substantial public interest; (b) is necessary for the purposes of the prevention or detection of any unlawful act; and (c) must necessarily be carried out without the explicit consent of the data subject being sought so as not to prejudice those purposes. (2) In this paragraph, "act" includes a failure to act." ('Unlawful act etc.')

[29] Of course the police may use any of the other conditions where appropriate.

And

Paragraph 10 which covers processing by the police in the exercise of their common law powers - "10. The processing is necessary for the exercise of any functions conferred on a constable by any rule of law." ('Conferred on a Constable')

Further conditions were identified in The Data Protection (Processing of Sensitive Personal Data) Order 2006 (Statutory Instrument 2068 of 2006). The Order specified that personal data about a criminal conviction or caution may be processed for the purpose of administering an account relating to the payment card (or for cancelling the payment card) used in the commission of one of the listed offences relating to indecent images of children and for which the data subject has been convicted or cautioned under the relevant legislation in England and Wales, Scotland or Northern Ireland.

The schedule 3 conditions likely to be of most relevance to the police are examined in more detail in the following subsections 3.2.5.2 to 3.2.5.7.

3.2.5.2 Schedule 3: 'Explicit Consent'

The first schedule 3 condition requires that the data subject has given his/her explicit consent to the processing of their sensitive personal data. This provision goes beyond that of consent under schedule 2 (see 3.2.4.2) in that in the case of sensitive personal data, the consent has to be 'explicit'.

The Information Commissioner's legal guidance advises:

'There is a distinction in the Act between the nature of the consent required to satisfy the condition for processing [schedule 2] and that which is required in the case of the condition for processing sensitive data [schedule 3]. The consent must be "explicit" in the case of sensitive data. The use of the word "explicit" and the fact that the condition requires explicit consent "to the processing of the personal data" suggests that the consent of the data subject should be absolutely clear. In appropriate cases it should cover the specific detail of the processing, the particular type of data to be processed (or even the specific information), the purposes of the processing and any special aspects of the processing which may affect the individual, for example, disclosures which may be made of the data.'

As with consent under schedule 2, ACPO recommends that explicit consent is not solely relied upon as a schedule 3 condition for processing sensitive personal data.

Where a police force intends to rely on this condition it is recommended to obtain the consent in writing in order that it can be shown that the consent was informed, clear, freely given and unambiguous.

3.2.5.3 Schedule 3: 'Vital Interests'

The third schedule 3 condition allows the processing of sensitive personal data where it is necessary:

(a) in order to protect the vital interests of the data subject or another person, in a case where consent cannot be given by or on behalf of the data subject, or the data controller cannot reasonably be expected to obtain the consent of the data subject, or;

(b) in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.

This condition appears wider than its 'cousin' under schedule 2 (see 3.2.4.4) in that it covers both the data subject and 'another person'.

In other respects it is narrower because it requires case-by-case consideration of consent issues. An example of where consent could not be given could be where the data subject was incapacitated or

absent. An example of where it would be unreasonable to obtain consent could be where the intention was to disclose a data subject's criminality to protect a third-party and seeking consent would be likely to seriously aggravate the situation. Finally, an example of where consent was 'unreasonably withheld' could be where the intention was to disclose a data subject's mental health condition to protect a third-party and consent had been withheld.

As with the schedule 2 condition the police are likely to adopt a less restrictive interpretation of 'vital interests' than that offered by the Information Commissioner.

Examples of its likely use within the policing context include:

The police appealing to the public for assistance in locating the whereabouts of a named dangerous offender at large and in doing so releasing some details of his/her criminal convictions.

Disclosure by the police of sensitive personal data relating to the health of an individual of concern to a medical practitioner.

3.2.5.4 Schedule 3: 'Legal Proceedings'

The sixth schedule 3 condition allows the processing of sensitive personal data where it is:

(a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings);

(b) is necessary for the purpose of obtaining legal advice, or;

(c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

The Information Commissioner's legal guidance advises:

"The Commissioner's view is that (c) above is of limited scope and data controllers should adopt a narrow interpretation and rely upon another Schedule 3 condition if there is any doubt as to whether it applies. In particular, it should not be used to construct a legal right where none exists."

These grounds cover much of the processing of personal data by the police. For example:

Processing by the police of sensitive personal data relating to suspects for the purposes of prosecuting those individuals;

Disclosure of sensitive personal data by the police to a solicitor in order to obtain legal advice and opinion for an employment tribunal case.

3.2.5.5 Schedule 3: 'Public Functions'

The seventh schedule 3 condition allows the processing of sensitive personal data where it is necessary for:

(a) for the administration of justice;

(b) for the exercise of any functions conferred on any person (including a constable) by or under an enactment, or;

(c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department.

This is largely repetitious of the fifth schedule 2 condition (see 3.2.4.5), except that the rarely used fourth provision in schedule 2 is not included in the schedule 3 version. Compliance with the schedule 3 condition should not be problematic if compliance is achieved with its narrower schedule 2 counterpart.

3.2.5.6 Schedule 3: 'Unlawful act etc.'

Paragraph 1 of Statutory Instrument 2000 No. 417 The Data Protection (Processing of Sensitive Personal Data) Order 2000 allows the processing of sensitive personal data where the processing is in the substantial public interest, is necessary for the prevention or detection of any unlawful act, and must necessarily be carried out without the explicit consent of the data subject being sought so not to prejudice those purposes. The term 'act' includes a failure to act.

The use of the term 'unlawful' means that the act or omission is not restricted to criminal activity, but also covers breaches of civil obligations. This condition can only be relied upon where there would be a real prejudice to the purpose if the data subject was to be told of the processing and was asked to consent.

The condition tends to overlap with those available under Schedule 3 paragraphs 6 and 7 and that under paragraph 10 of Statutory Instrument 2000 No. 417 The Data Protection (Processing of Sensitive Personal Data) Order 2000 – though the fact that it extends beyond criminal activity may prove useful.

The following is an example of its likely use within the policing context:

> *The police investigating an individual suspected of planning to commit serious criminal offences where seeking consent to process his/her personal data would prejudice that investigation.*

3.2.5.7 Schedule 3: 'Conferred on a Constable'

Paragraph 10 of Statutory Instrument 2000 No. 417 The Data Protection (Processing of Sensitive Personal Data) Order 2000 allows the processing of sensitive personal data where necessary for the exercise of any functions conferred on a constable by any rule of law.

This appears to be a broad 'catch-all' that is likely to be used where sensitive personal data is processed for operational policing purposes but does not fit under any of the other schedule 3 conditions. It demands that the processing is necessary for activity derived from a specific legal power.

3.3 The Second Principle

3.3.1 Second Principle: Introduction

The second principle requires that, subject to exemptions[30], personal data shall be obtained only for one or more specified and lawful purpose(s) and shall not be further processed in any manner incompatible with that purpose or those purposes[31].

The 'specified' element of the second principle may be achieved either through a 'fair processing notice' given by the police force to the data subject in accordance with the fair processing requirements (see 3.2.3.1 to 3.2.3.4) or, in a notification given to the Commissioner under part III of the Act (see 3.3.2).

3.3.2 Second Principle: Notification

The Act requires that data controllers must notify their processing of personal data to the Information Commissioner. Failure to do so is an offence. Notification also achieves the 'specified' element of the second principle.

The ACPO Data Protection Portfolio produced a standard 'Notification' to fulfil the Act's requirements several years ago. This has been utilised by the vast majority of police forces. That Notification will continue to be used, subject to a minor amendment required by the Freedom of Information Act 2000 which requires police forces to include within the Notification a statement to the effect that the police

[30] Exemptions are summarised in appendix b.
[31] DPA Schedule 1 part 2 paragraphs 5 and 6 provides further interpretation of the second principle.

force is a 'Public Authority'.

It may be necessary from time to time for the Notification to be amended. Proposals to amend it will be submitted to the ACPO Data Protection Portfolio for consideration/rejection/ approval on behalf of all police forces.

The inclusion of a description of a purpose, source, data subject, data class, recipient or transfer within the Notification must not be regarded as an automatic 'green light' which enables processing to go ahead without any further consideration. In all cases the processing must be assessed against all the principles, with the Notification merely regarded as a high-level public description of processing that a police force may undertake.

3.3.3 Second Principle: Incompatible Use

The interpretation of the second principle[32] explains that in deciding whether any disclosure of personal data is compatible with the purpose(s) for which the personal data was obtained, consideration will be given to the purpose(s) for which the personal data is intended to be processed by any person to whom they are disclosed. Such decisions cannot be made retrospectively by data controllers once the data has been obtained.

The use of the term 'incompatible' suggests that the principle would be breached if the use of personal data was contradictory to the purposes it was obtained. However, if the use was merely different to that for which it was obtained (as opposed to contradictory) then the provision would be likely to be satisfied providing any new compatible purpose was notified to the data subject in accordance with the fairness requirements of the first principle.

The following is provided as an example within the policing arena of where use was likely to be compatible:

> *Personal data is obtained by the police from suspects in the course of an investigation into a specific offence in accord with the force's Notification. The personal data is subsequently disclosed to another police force for investigations into other offences.*

Incompatible use is likely to occur in the following scenarios:

> *Address details of police employees, originally obtained and held by the police force for staff administration purposes are disclosed to an outside organisation for subsequent direct marketing use; or the police force uses the details to send advertising material to employees.*

3.4 Disputes and Complaints

Police forces must develop processes to resolve disputes or complaints regarding the fair and lawful processing or otherwise of personal data.

3.5 Fair & Lawful Processing: Checklist

The following is provided as a brief aide-memoir when considering the first and second principles in relation to a proposed processing operation.

Assessing Fair and Lawful Processing
What is the purpose(s) of the processing?
What processing operations are involved?
Who is the data controller?
Who else processes the personal data? Their status?
What personal data is processed?

[32] See DPA Schedule 1 part 2 paragraph 6.

What sensitive personal data is processed?
What are the lawful grounds for processing?
Are there any prohibitions from processing?
Can a schedule 2 (& 3 if needed) condition be met?
How will the processing be fair?
How will the 'fair processing requirements' be met?
Which exemptions can be employed?
Has the processing been notified?
Is the processing compatible with the original purpose(s)?

3.6 Standards

Standard	Source
Police force has considered the need for 'fair processing notices' in the scenarios described.	3.2.3.4
Police force has notified to the Information Commissioner using the standard Notification.	3.3.2
Police force has established a process to resolve fair and lawful processing disputes and complaints.	3.4

4 Privacy Impact Assessments (PIAs)

4.1 Overview

This guidance provides a process which will enable:

the collection of sufficient information about the new process/initiative/IT system to allow a decision to be made as to whether a PIA should be conducted;

a decision about whether the PIA should be small scale or full scale;

a PIA report to be drafted;

any privacy risks to be identified, documented and considered.

4.2 Privacy Impact Assessments

4.2.1 Assumptions

It is assumed that:

Any new project/initiative will be subject to force policy which requires the project/initiative to be formally approved. This PIA guidance is based on that surmise. If a force does not have this process in place e.g. when making significant changes to a process/IT system, it is suggested that those departments which may undertake work in this area are made aware of PIAs and this guidance;

Any national Police system or project will consider a PIA as part of their initial phase and it will not be incumbent on forces to undertake one prior to roll out locally – that is too late in any event for a PIA to be conducted.

4.2.2 Recommendations

It is recommended that forces incorporate the PIA process into their project management policy/process.

If more PIA detail is required, please refer to the Information Commissioner's website.

4.2.3 Introduction

A PIA is a process which enables Organisations to identify and address the likely privacy impact of new initiatives and projects (see PIA Chapter: Appendix A on page 35). Whilst a PIA considers privacy issues on a wider scale than data protection compliance considerations, undertaking a PIA does not negate the need for data protection and information security compliance to be undertaken. Nor does a Data Protection compliance check cover all PIA aspects.

4.2.4 What are Privacy Issues?

Privacy of personal information (Data Protection Act 1998);

Privacy of the person (e.g. body searches, body scanning);

Privacy of personal behaviour (observations of what individuals do);

Privacy of personal communication.

4.2.5 Key Messages about PIAs

The key messages for police forces are as follows:

A PIA is not always necessary – especially a full scale one – so don't assume that one must be done for every project;

Start the PIA at a stage when it can influence a project;

The consultation phase is the key, so the focus should be on identifying the appropriate internal and external stakeholders and consulting effectively;

Use whatever consultation and reporting format works for the force;

Don't conclude that there are no privacy risks with a project. The report should show what risks were identified and how they will be mitigated. A force should be arguing why an acceptable level of risk is justified, not ignoring risks that are there.

4.2.6 Why undertake a PIA?

Undertaking a PIA will assist forces by:

Increasing public confidence in the way in which forces collect and use personal information;

Allowing forces to consider the legal basis for the new system, any obligation in relation to the collection of the personal data and any prohibitions on the use of that information;

Preventing problems arising and hence avoid subsequent expense and disruption;

Assisting with risk management;

Protecting the reputation of the force.

4.2.7 Do all IT new process/initiative/IT systems require a full PIA?

No – an initial assessment of the privacy risk should be undertaken to determine what scale of PIA is necessary (see PIA Chapter: Appendices B and D on pages 36 and 46 respectively):

Full Scale PIA – an in-depth internal assessment of privacy risks and liabilities e.g. does a new IT system now require the use of personal data whereas previously it was purely statistical in nature

Small Scale PIA – a less formalised process e.g. replacement or enhancement so an existing personal data system or a proposal to collect personal data from a new source.

4.2.8 When should a PIA be undertaken?

If a force is introducing a new process/initiative or IT system or is making significant changes to a process/IT system, that has implications for the use of personal information, a PIA should be considered.

It could be undertaken at the same time as other assessment e.g. an equality impact assessment, or it could be considered separately. Initial data protection and information considerations are identified early in a project stage, the compliance checks are usually undertaken once the design has reached a detailed stage.

Initial PIA work should be undertaken prior to going to tender (i.e. at the project initiation phase or its equivalent or the business case stage - certainly before decisions are made about the IT system/process/initiative). It may be appropriate to insert the initial PIA within a relevant contract.

To be effective, the PIA should be reviewed regularly at each new project phase and a review undertaken e.g. at a stage review (PRINCE methodology).

A PIA should not be undertaken retrospectively on an IT system or process already in place. Initial PIA reports should be revisited during various stages of the process.

4.2.9 Examples of new initiatives/IT systems

Home Office Data Hub (staff data), Crime Mapping (victim data), use of social networking sites, new or significantly changing an IT system or business process which will capture new categories/types of personal data.

4.2.10 What should a PIA document look like?

There is no set format and is likely to depend on individual force requirements. It is important to log issues raised and how they have been addressed, so should include the privacy risks and countermeasures (this supports legal compliance and will also be a reference document for any media statements required in the future). The final report should refer back to the initial PIA and reviews, provide an outline of the outstanding PIA risks and refer to previous mitigated risks (list). Further information can be found in PIA Chapter: Appendix C on page 44).

4.2.11 Who should conduct a PIA and who should be involved in the process?

The project manager or similar should conduct the PIA.

4.2.12 Consultation

It is for the individual force to decide about who they consult. Who to consult is also dependant on the reason for the use and the type of the information being collected. What is important is what can be gained by such consultation e.g. information which will prevent problems arising at a later stage which could result in cost and disruption.

Must be consulted	**Should be consulted:**
Subject Matter Experts (SMEs), e.g Data Protection Officer	Users
Information Security Officer	Federation/UNISON/Supts Association
Record Manager	Owner of the System/Process/Initiative (and any owners of systems it may impact on)
IT Manager (if relevant)	Partner Agencies
	Public (dependant on type)
	Regulatory Authorities e.g. ICO

4.2.13 Responsibilities

SIRO (Senior Information Risk Owner) should:

ensure a PIA is completed at appropriate stages of a project as it informs on risk assessments and risk management;

accept/reject any risk from the PIA document.

Project Owner:

identify the individual who will conduct the PIA;

ensure sufficient resources are provided to the PIA process;

complete the PIA tasks at appropriate times;

responsible for the project risk register which should include the PIA risks.

PIA responsible person:

complete the PIA in accordance with local force policy;

draft the PIA report.

PIA Chapter: Appendix A

Privacy Impact Assessment (PIA) Workflow

Prepare an initial assessment of the project/initiative that includes a project outline, stakeholder analysis and environmental scan

↓

Discuss with DPO, ISO & RM who will advise if more information required

↓

Initial screening with DPO, ISO & RM informed by discussions

↓

Carry out the PIA screening process (PIA Chapter: Appendix B and flowchart) in consultation with DPO, ISO & RM informed by discussions to identify whether full or small scale PIA required, and whether legislative compliance checks should be integrated into the overall project schedule. It would be appropriate to highlight any potential legislative compliance issues that may be apparent at this early stage, although the full legislative compliance checks are normally carried out at a later stage of the project after the system design, business processes and rules have been specified sufficiently so that they can be assessed for compliance with the law.

↓

Preliminary PIA report PIA Chapter: Appendix C
(to allow formal decision regarding small scale or full scale PIA).

↓

Complete Small Scale/Full Scale PIA to include drafting report

↓

Regular review of PIA plus data protection & information security requirements

↓

Consideration of risks from the PIA/DP and information security reviews to be included with Force risk register

↓

PIA document plus risks presented to SIRO

PIA Chapter: Appendix B

Privacy Impact Assessment (PIA)

The answers to these questions will determine the scale of PIA needed (Full, Small or None), and whether a Privacy Law and/or Data Protection Act compliance check is also required.

Project:			
	Step 1 - Criteria for Full-Scale PIA	**Yes**	**No**
	Technology		
1	**Does the project apply new or additional information technologies that have substantial potential for privacy intrusion?** *Examples include, but are not limited to, smart cards, radio frequency identification (RFID) tags, biometrics, locator technologies (including mobile phone location, applications of global positioning systems (GPS) and intelligent transportation systems), visual surveillance, digital image and video recording, profiling, data mining, and logging of electronic traffic.*	☐	☐
	Identity		
2	**Does the project involve new identifiers, re-use of existing identifiers, or intrusive identification, identity authentication or identity management processes?** *Examples of relevant project features include a digital signature initiative, a multi-purpose identifier, interviews and the presentation of identity documents as part of a registration scheme, and an intrusive identifier such as biometrics. All schemes of this nature have considerable potential for privacy impact and give rise to substantial public concern and hence project risk.*	☐	☐
3	**Might the project have the effect of denying anonymity and pseudonymity, or converting transactions that could previously be conducted anonymously or pseudonymously into identified transactions?** *Many Police functions cannot be effectively performed without access to the client's identity. On the other hand, many others do not require identity. An important aspect of privacy protection is sustaining the right to interact with organisations without declaring one's identity.*	☐	☐
	Multiple Organisations		
4	**Does the project involve multiple organisations, whether they are government agencies (eg in 'joined-up government' initiatives) or private sector organisations (eg as outsourced service providers or as 'business partners')?** *Schemes of this nature often involve the breakdown of personal data silos and identity silos, and may raise questions about how to comply with data protection legislation. This breakdown may be desirable for fraud detection and prevention, and in some cases for business process efficiency. However, data silos and identity silos are of long standing, and have in many cases provided effective privacy protection. Particular care is therefore needed in relation to preparation of a business case that justifies the privacy invasions of projects involving multiple organisations. Compensatory protection measures should be considered.*	☐	☐
	Data		
5	**Does the project involve new or significantly changed handling of personal data that is of particular concern to individuals?** *The Data Protection Act (schedule 2) identifies a number of categories of 'sensitive personal data' that require special care. These include racial and ethnic origin, political opinions, religious beliefs, trade union membership, health conditions, sexual life, offences and court proceedings.* *There are other categories of personal data that may give rise to concerns, including financial data, particular data about vulnerable individuals, and data which can enable identity theft.* *Further important examples apply in particular circumstances. The addresses and phone-numbers of a small proportion of the population need to be suppressed, at least at particular times in their lives, because such 'persons at risk' may suffer physical harm if they are found.*	☐	☐

	Step 1 - Criteria for Full-Scale PIA	Yes	No
	Technology		
1	**Does the project apply new or additional information technologies that have substantial potential for privacy intrusion?** *Examples include, but are not limited to, smart cards, radio frequency identification (RFID) tags, biometrics, locator technologies (including mobile phone location, applications of global positioning systems (GPS) and intelligent transportation systems), visual surveillance, digital image and video recording, profiling, data mining, and logging of electronic traffic.*	☐	☐
	Identity		
2	**Does the project involve new identifiers, re-use of existing identifiers, or intrusive identification, identity authentication or identity management processes?** *Examples of relevant project features include a digital signature initiative, a multi-purpose identifier, interviews and the presentation of identity documents as part of a registration scheme, and an intrusive identifier such as biometrics. All schemes of this nature have considerable potential for privacy impact and give rise to substantial public concern and hence project risk.*	☐	☐
3	**Might the project have the effect of denying anonymity and pseudonymity, or converting transactions that could previously be conducted anonymously or pseudonymously into identified transactions?** *Many Police functions cannot be effectively performed without access to the client's identity. On the other hand, many others do not require identity. An important aspect of privacy protection is sustaining the right to interact with organisations without declaring one's identity.*	☐	☐
	Multiple Organisations		
4	**Does the project involve multiple organisations, whether they are government agencies (eg in 'joined-up government' initiatives) or private sector organisations (eg as outsourced service providers or as 'business partners')?** *Schemes of this nature often involve the breakdown of personal data silos and identity silos, and may raise questions about how to comply with data protection legislation. This breakdown may be desirable for fraud detection and prevention, and in some cases for business process efficiency. However, data silos and identity silos are of long standing, and have in many cases provided effective privacy protection. Particular care is therefore needed in relation to preparation of a business case that justifies the privacy invasions of projects involving multiple organisations. Compensatory protection measures should be considered.*	☐	☐
	Data		
5	**Does the project involve new or significantly changed handling of personal data that is of particular concern to individuals?** *The Data Protection Act (schedule 2) identifies a number of categories of 'sensitive personal data' that require special care. These include racial and ethnic origin, political opinions, religious beliefs, trade union membership, health conditions, sexual life, offences and court proceedings.* *There are other categories of personal data that may give rise to concerns, including financial data, particular data about vulnerable individuals, and data which can enable identity theft.* *Further important examples apply in particular circumstances. The addresses and phone-numbers of a small proportion of the population need to be suppressed, at least at particular times in their lives, because such 'persons at risk' may suffer physical harm if they are found.*	☐	☐

6	**Does the project involve new or significantly changed handling of a considerable amount of personal data about each individual in the database?** *Examples include intensive data processing such as Staff HR, Crime data, Intelligence data.*	☐	☐
7	**Does the project involve new or significantly changed handling of personal data about a large number of individuals?** *Any data processing of this nature is attractive to organisations and individuals seeking to locate people, or to build or enhance profiles of them.*	☐	☐
8	**Does the project involve new or significantly changed consolidation, inter-linking, cross-referencing or matching of personal data from multiple sources?** *This is an especially important factor. Issues arise in relation to data quality, the diverse meanings of superficially similar data-items, and the retention of data beyond the very short term.*	☐	☐
	Exemptions and Exceptions		
9	**Does the project relate to data processing which is in any way exempt from legislative privacy protections?** *Examples include law enforcement and national security information systems and also other schemes where some or all of the privacy protections may be negated by legislative exemptions or exceptions.*	☐	☐
10	**Does the project's justification include significant contributions to public security measures?** *Measures to address concerns about critical infrastructure and the physical safety of the population usually have a substantial impact on privacy. Yet there have been tendencies in recent years not to give privacy its due weight. This has resulted in tensions with privacy interests, and creates the risk of public opposition and non-adoption of the programme or scheme.*	☐	☐
11	**Does the project involve systematic disclosure of personal data to, or access by, third parties that are not subject to comparable privacy regulation?** *Disclosure may arise through various mechanisms such as information sharing with other agencies or outsourcing of aspects of the data-handling to sub-contractors.* *Third parties may not be subject to comparable privacy regulation because they are not subject to the provisions of the Data Protection Act or other relevant statutory provisions, such as where they are in a foreign jurisdiction. Concern may also arise in the case of organisations within the UK which are subsidiaries of organisations headquartered outside the UK.*	☐	☐

The answers to questions 1 – 11 need to be considered as a whole to determine whether a full-scale PIA is warranted, and if so, whether the scope of the PIA should be wide-ranging or focused on a particular aspect of the project.

Full-Scale PIA required?	**Yes**	**No**
	☐	☐

If a full-scale PIA is not required, proceed to Step 2 - Criteria for Small-Scale PIA

If a full-scale PIA is required, what should be its scope?

Proceed to Step 3 - Criteria for Privacy Law Compliance Check

	Project:		
	Step 2 - Criteria for Small-Scale PIA	**Yes**	**No**
	Technology		
12	**Does the project involve new or inherently privacy-invasive technologies?** *Examples of such technologies include, but are not limited to, smart cards, radio frequency identification (RFID) tags, biometrics, locator technologies (including mobile phone location, applications of global positioning systems (GPS) and intelligent transportation systems), visual surveillance, digital image and video recording, profiling, data mining, and logging of electronic traffic.* *Technologies that are inherently intrusive, and technologies that are new and sound threatening, excite considerable public concern, and hence represent project risk.* *In order to answer this question, considerations include:* • *whether all of the information technologies that are to be applied in the project are already well-understood by the public;* • *whether their privacy impacts are all well-understood by the organisation, and by the public;* • *whether there are established measures that avoid negative privacy impacts, or at least reduce them to the satisfaction of those whose privacy is affected;* • *and whether all of those measures are being applied in the design of the project.*	☐	☐
	Justification		
13	**Is the justification for the new data-handling unclear or unpublished?** *Individuals are generally much more accepting of measures, even measures that are somewhat privacy-intrusive, if they can see that the loss of privacy is balanced by some other benefits to themselves or society as a whole. On the other hand, vague assertions that the measures are needed 'for security reasons', or 'to prevent fraud', are much less likely to calm public disquiet.*	☐	☐
	Identity		
14	**Does the project involve an additional use of an existing identifier?**	☐	☐
15	**Does the project involve use of a new identifier for multiple purposes?**	☐	☐
16	**Does the project involve new or substantially changed identity authentication requirements that may be intrusive or onerous?** *The public understands that an identifier enables an organisation to collate data about an individual, and that identifiers that are used for multiple purposes enable data consolidation. They are also aware of the increasingly onerous registration processes and document production requirements imposed by organisations in recent years. From the perspective of the project manager, these are warning signs of potential privacy risks.*	☐	☐
	Data		
17	**Will the project result in the handling of a significant amount of new data about each person, or significant change in existing data-holdings?**	☐	☐
18	**Will the project result in the handling of new data about a significant number of people, or a significant change in the population coverage?**	☐	☐
19	**Does the project involve new linkage of personal data with data in other collections, or significant change in data linkages?** *The degree of concern about a project is higher where data is transferred out of its original context. The term 'linkage' encompasses many kinds of activities, such as the transfer of data, the consolidation of data-holdings, the storage of identifiers used in other systems in order to facilitate the future searches of the current content of records, the act of fetching data from another location (eg to support so-called 'front-end verification'), and the matching of personal data from multiple sources.*	☐	☐

	Data Handling		
20	**Does the project involve new or changed data collection policies or practices that may be unclear or intrusive?**	☐	☐
21	**Does the project involve new or changed data quality assurance processes and standards that may be unclear or unsatisfactory?**	☐	☐
22	**Does the project involve new or changed data security arrangements that may be unclear or unsatisfactory?**	☐	☐
23	**Does the project involve new or changed data access or disclosure arrangements that may be unclear or permissive?**	☐	☐
24	**Does the project involve new or changed data retention arrangements that may be unclear or extensive?**	☐	☐
25	**Does the project involve changing the medium of disclosure for publicly available information in such a way that the data becomes more readily accessible than before?**	☐	☐
	Exemptions		
26	**Will the project give rise to new or changed data-handling that is in any way exempt from legislative privacy protections?**	☐	☐

Where the answers to questions 12 - 26 are "Yes", consideration should be given to the extent of the privacy impact and the resulting project risk. The greater the significance, the more likely that a small-scale PIA is warranted.

If only one or two aspects give rise to privacy concerns, a small-scale PIA may still be justified. In these circumstances the PIA process should be designed to focus on the areas of concern. If, on the other hand, multiple questions are answered "Yes", a more comprehensive assessment is appropriate.

	Yes	No
Small-Scale PIA required?	☐	☐

If a small-scale PIA is not required proceed to Step 3 - Criteria for Privacy Law Compliance Check

If a small-scale PIA is required, what should be its scope?

Proceed to Step 3 - Criteria for Privacy Law Compliance Check

The answers to these questions will determine whether a privacy law compliance check will be required.

	Project:		
	Step 3 - Criteria For Privacy Law Compliance Check	**Yes**	**No**
27	**Does the project involve any activities (including any data handling), that are subject to privacy or related provisions of any statute or other forms of regulation, other than the Data Protection Act?** *In particular, the following laws and other forms of regulation should be considered, but the list may not be exhaustive.* • *The Human Rights Act, in particular Schedule 1, Article 8 (right to respect for private and family life) and Article 14 (prohibition of discrimination).* • *The Regulation of Investigatory Powers Act 2000 (RIPA) and Lawful Business Practice Regulations 2000.* • *The Privacy and Electronic Communications Regulations 2003 (PECR).* • *The Data Retention (EC Directive) Regulations 2007.* • *In the case of government agencies, the statutes under which the agency or programme operates.* • *Statutes that impose regulatory conditions on the manner in which the organisation operates.* • *Sectoral legislation, eg Financial Services and Markets Act 2000.* • *Statutory codes, eg the Information Commissioner's CCTV code of practice.* *Where projects are cross-jurisdictional the law of more than one country may be involved and other legal provisions may also need to be considered.*	☐	☐
28	**Does the project involve any activities (including any data handling) that are subject to common law constraints relevant to privacy?** *In particular, the following should be considered:* • *confidential data relating to a person, as that term would be understood under the common law of confidence;* • *the tort of privacy as it develops through case law*	☐	☐
29	**Does the project involve any activities (including any data handling) that are subject to less formal good practice requirements relevant to privacy?** *In particular, the following should be considered:* • *industry standards, eg the BS ISO / IEC 17799:2005 Information Security Standard;*	☐	☐

If any of the questions 27 – 29 are answered "Yes", then a privacy law compliance check should be integrated into the project schedule.

Proceed to <u>Step 4</u> - <u>Criteria for Data Protection Compliance Check</u>

The answers to these questions will determine whether a Data Protection compliance check will be required.

Project:	

	Step 4 - Criteria for Data Protection Act Compliance Check	**Yes**	**No**
30	**Does the project involve the handling of any data that is personal data, as that term is used in the Data Protection Act?** *'Personal data' means data which relate to a living individual who can be identified:* *(a) from those data, or* *(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual (Data Protection Act, s.1).* *Before proceeding to Data Protection Compliance checking, it is advisable to return to the screening process and review the outcomes of the four steps.* *Note that, where a PIA is needed, it should be commenced at an early stage of the overall project, whereas compliance checking activities are usually conducted only once a fairly mature stage of business process design has been reached.*	☐	☐

If question 30 is answered "Yes", then a Data Protection compliance check should be integrated into the project schedule.

Note that compliance checking activities are usually conducted reasonably late in the overall project schedule, once detailed information about business processes and business rules is available.

PIA Screening Process completed by:

Name: ..... Signature: ..... Date: .....

Reviewed by:

Name: ..... Signature: ..... Date: .....

Name: ..... Signature: ..... Date: .....

PIA Chapter: Appendix C

Preliminary Privacy Impact Assessment (PIA) Report

Purpose

The purpose of the report is to document the conduct of, and recommendations arising from the preliminary PIA process. The report is for the consideration of the Senior Information Risk Officer and should identify:

potential privacy and data protection risks related to the proposed project;
the scale of PIA required, (Full, Small or None);
the scope of the PIA if one is required;
whether a privacy law compliance check should be integrated into the project schedule;
whether a Data Protection Act compliance check should be integrated into the project schedule.

Format

The format of the report should be in accordance with local requirements. Where privacy and data protection risks have been identified, it is recommended that these are recorded in a format suitable for incorporation into the Project Risk Register and / or Force Risk Register as appropriate.

Protective Marking – would suggest this is marked at RESTRICTED when complete – however that is for the originator to decide.

Structure and Content

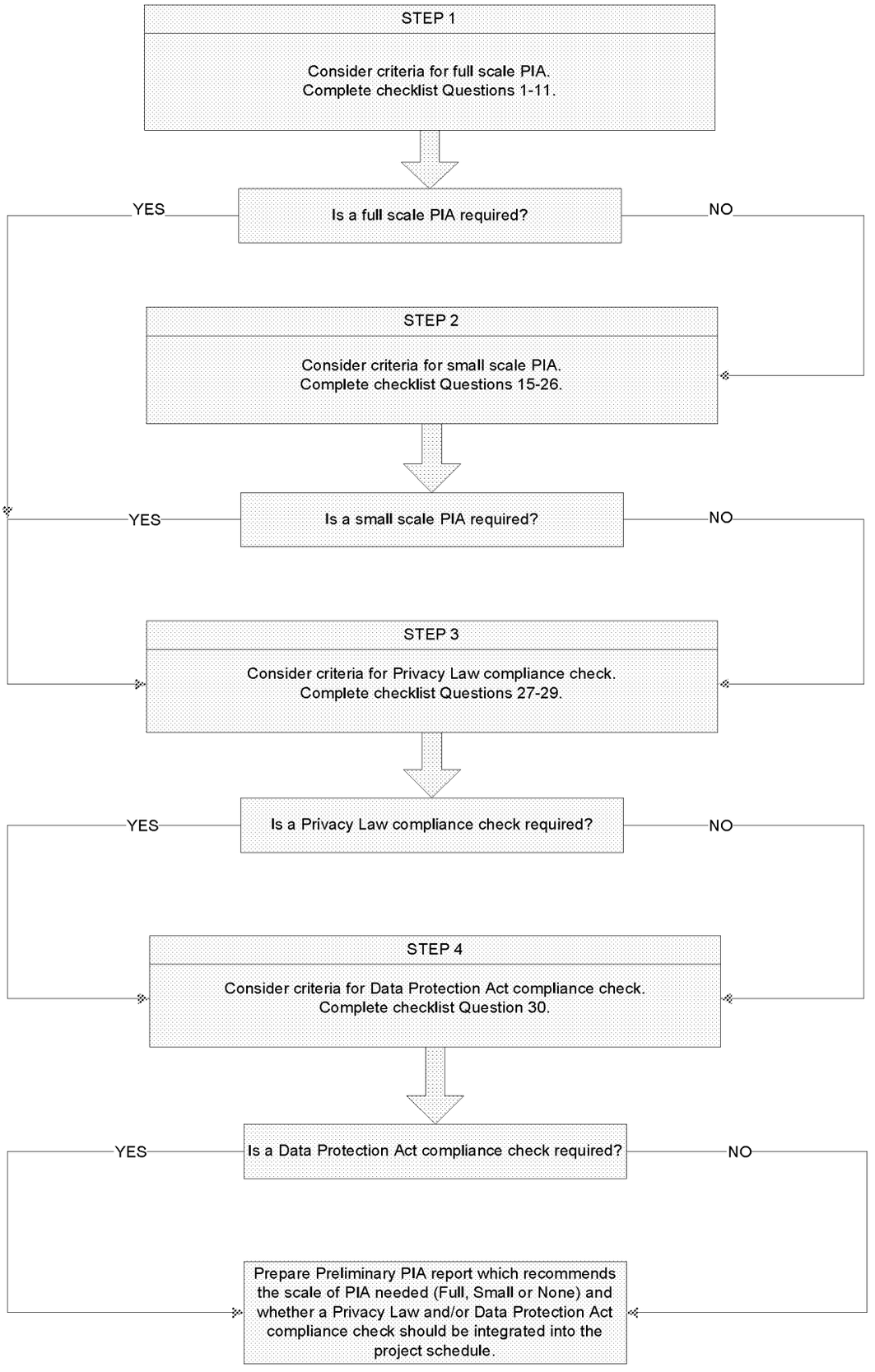
The following elements are recommended and the level of detail should be adapted to suit the scope and complexity of the project, and the level of risk identified.

Executive summary:	An overview of the preliminary PIA process, including project outline, stakeholder analysis, environmental scan, PIA screening results; and a summary of the main findings and recommendations.
Introduction:	The purpose of the preliminary PIA, the system/process to which it refers and any relationships with other internal/external systems/processes.
Project background:	Project description, purpose, scope, links to other projects, stakeholders, type(s) of information to be processed, the reasons for processing and related privacy aspects.
Legislative and policy authorities	Record all known legislative and policy authorities that are relevant to the project
Description of personal information:	What specific information is to be processed and how will it flow internally and externally. How will it be collected, used, stored, transferred and disclosed. What are the arrangements regarding subject access and data quality Data elements and data flows should be described and / or mapped in relation to the identified stakeholders.
Potential privacy risks:	Privacy risks that have been identified and how these will affect stakeholders and the aims of the project. The relevant seriousness of these risks and steps that might be taken to remove, mitigate or manage those risks.

Potential data protection risks	Data protection risks that have been identified and how these will affect stakeholders and the aims of the project. The relevant seriousness of these risks and steps that might be taken to remove, mitigate or manage those risks.
Security requirements:	Measures to protect personal information from loss and unauthorised access, use, modification or disclosure. Measures to protect personal information which is transferred to other locations, and /or will be handled by external agencies. Review retention and disposal arrangements. Breach management policy.
Environmental:	Detail any consideration of prior PIAs within the organisation or in other organisations, consultations with other professional bodies, privacy regulators etc.
Recommendations:	These will be derived from the PIA screening process and should address whether a PIA required, and if so what scale (Full or Small) and scope is appropriate. The recommendations should also address whether a privacy law compliance check and /or Data Protection Act compliance check should be integrated into the project schedule. If a PIA is to be conducted the recommendations should include an indication of future activities, timescales and resource requirements for conducting the PIA. Where a PIA is needed it should be commenced at an early stage of the overall project, whereas compliance checking activities are usually conducted at a much later stage, once detailed information about the business process design and business rules are available.

Appendix D

PIA Screening Process



5 Data Quality, Review, Retention and Disposal

5.1 Overview

The first part of this chapter examines data quality considerations which arise from the third and fourth principles and their application across the police service. The chapter also covers the fifth principle concepts of review, retention and disposal.

A checklist is provided towards the end of the chapter, which is designed to assist navigation through the third to fifth principles.

5.2 Data Quality

5.2.1 Introduction

The third principle of the Act states that personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed. Unlike the first and second principles there are no interpretative provisions for this principle.

The fourth principle states that personal data shall be accurate and, where necessary, kept up to date.

Limited exemptions are available from the third and fourth principles and are summarised at appendix b.

5.2.2 Third Principle

To comply with this principle, the police will seek to identify the minimum amount of personal data that is required in order properly to fulfil their purpose(s). That personal data must also be adequate for the purpose(s). Clearly there is a crucial requirement to define the purpose(s) of the processing.

The police will regularly monitor compliance with this principle as changes in circumstances or failure to keep the information up to date may mean that personal data that was originally compliant becomes non-compliant.

Notwithstanding the Act there will be significant practical operational benefits for the police if the personal data it processes is adequate, relevant and not excessive.

5.2.2.1 Relevance and Excessiveness

To establish relevance, a necessity test will identify the minimum amount of personal data that is required to achieve the specific purpose(s).

Some processing operations, such as staff administration or police investigations, may require the use of a great deal of a particular data subject's personal data. In other circumstances only a minimal amount is necessary.

It is excessive to hold a class of data on all individuals where that particular item of data is only relevant in certain individual cases.[33]

Where personal data is processed for the purpose of criminal intelligence or during the course of a major investigation, appropriate guidance must be given to those having responsibility for deciding what will and what will not be recorded.

The police will adopt practices to ensure that personal data that fails to meet the requisite criteria for

33 This approach has been endorsed by the Data Protection Tribunal in the context of the 1984 Act in the case of Runnymede Borough Council CCRO and Others v The Data Protection Registrar (November 1990).

relevancy is either brought up to those criteria, or rejected. When determining relevance consideration must be given to the necessity and proportionality of processing the personal data.

Personal data must not be excessive in relation to the purpose for which it is held. It is difficult to argue that irrelevant information is not also excessive information.

If personal data is kept for longer than necessary (see fifth principle at 5.3.1) then it is likely to be both irrelevant and excessive.

5.2.2.2 Adequacy

All personal data processed by police forces must be sufficient for the purpose(s) for which it is used or likely to be used. The personal data must be clear in meaning and sufficient for others to understand at the present time and in the future.

Particular care must be taken to ensure that records of investigations are recorded in a way that means that subsequent enquirers accessing those records are afforded a complete picture of those investigations. For example:

> *Where a criminal investigation had been discontinued it is likely to be appropriate to record the rationale behind such a decision in case the matter later becomes a consideration when the personal data is accessed in another investigation or through a vetting process – there may be some significance as to whether the investigation was discontinued 'on a technicality', or because the aggrieved was not credible, or that the aggrieved did not wish to pursue the case.*

Those creating personal data must ensure that it is adequate, unambiguous and professionally worded. Opinions must be distinguishable from matters of fact.

Measures will be put in place to ensure that personal data held on police systems relating to one individual cannot be confused with that of another individual with the same name. This may be achieved by the inclusion of additional identifiers, such as date of birth and/or descriptive information.

Adequacy will also be achieved through the use of common data standards which may mean, for example, that the police record home addresses, descriptive information and other personal data in a format which assists interoperability of, and transfer between, different police information systems.

Police forces will comply with the requirements of the ACPO National Intelligence Model and all criminal intelligence will be graded using a standard evaluation system, which gives an indication of the quality of the information, the reliability of the source of the information and provides guidance on the subsequent use of that information.

5.2.3 Fourth Principle

As with the third principle, compliance with this principle has obvious operational benefits for the police.

The principle has two elements. The first, requiring accuracy of personal data, is unconditional, while the second element only requires the personal data to be kept up to date 'where necessary'.

5.2.3.1 Accuracy

Great care must be exercised in the collection of personal data. All staff, when recording personal data, must ensure that it is accurately recorded and where desirable its source is readily available. Where there is any doubt regarding accuracy, information must be clarified with the source.

Police forces must adopt procedures to prevent factual inaccuracies being entered onto police information systems.

This may be achieved by: -

Ensuring as far as possible that the source of the personal data is reliable;

Taking steps to verify the personal data if possible with another source or if reasonable, with the data subject, at the time of collection or at another convenient opportunity;

Using automatic validation procedures to ensure procedures for data entry and the information system itself does not introduce inaccuracies;

Using constrained fields in computer databases.

Where inaccuracies come to light, the police must take steps to lessen the damage or distress caused to the data subject or any other person by:

Ensuring the inaccurate personal data is corrected as soon as possible;

Passing the corrected personal data to any third-party to whom the inaccurate personal data may had already been disclosed;

Ensuring any other consequences which may have arisen before the personal data was corrected have been acted upon to minimise the damage or distress;

Acting on reports of inaccuracies received from other organisations or individuals.

Section 70(2) of the Act explains that personal data is 'inaccurate' if it is incorrect or misleading as to any matter of fact. Consequently, personal data that is presented as an opinion and does not claim to be fact cannot be challenged on the grounds of inaccuracy.

The interpretation provisions[34] provide that there is no breach of the accuracy requirement where the police have accurately recorded 'erroneous' information received from the data subject or someone else and have taken reasonable steps to ensure its accuracy. If the data subject has notified the police of their opinion of its inaccuracy, the personal data indicates that fact. The following is an example of this in the policing context:

A data subject disputes the accuracy of personal data supplied by a third-party to the police which is now held in an intelligence record. When the police recorded the personal data reasonable steps were taken to ensure its accuracy. In such circumstances, where the police are satisfied they have accurately recorded what may have originally been an allegation of something that did occur the police force will append the record explaining the accuracy dispute and the data subject's views.

The extent to which such 'reasonable steps' are necessary are a matter for each individual case and depend upon the nature of the personal data and the consequences of the inaccuracy for the data subject.

Under section 14 a court may order the police to rectify, block, erase or destroy inaccurate data or information based upon it (see 7.6).

In order to help maintain accuracy standards police forces will institute a programme of data protection compliance audits, inspections and monitoring in accordance with the companion to this document, ACPO Data Protection Manual of Guidance Part 2: Audit; and the Information Commissioner's Audit Manual June 2001 (see 1.6).

5.2.3.2 Kept up-to-Date

The second part of the fourth principle, which refers to keeping personal data up to date, is qualified in that updating is only required 'where necessary'.

[34] DPA schedule 1 part 2 paragraph 7.

The purpose for which the data are held or used will be relevant in deciding whether such updating is required. If the personal data is intended to be used merely as an 'historical' record or snap shot in time then updating would be inappropriate. For example:

> *It is not necessary to amend the arrestee's home address recorded on his six month-old custody record when the police learn today that he/she has moved to a new address in the past week – though the police may wish to update any intelligence nominal record for the individual.*

However, sometimes it is important for the purpose that the personal data reflects the data subject's current circumstances. Within the police service it is likely that such updating would be required in the following scenarios:

> *In order to keep up to date home address and next of kin details within a police force's collection of personnel records;*
>
> *To 'cancel' a stolen vehicle reports on the Police National Computer once the vehicle had been recovered.*

In the examples given above steps must be taken to ensure that the personal data is kept up to date, or when the personal data is used, account will be taken of the fact that circumstances may have changed.

When determining whether or not an item of personal data requires updating staff may consider the following:

> Is there a record of when the personal data was recorded or last updated?
>
> Are all those involved with the personal data aware that the personal does not necessarily reflect the current position?
>
> Are effective steps taken to update the personal data – for example, by checking back at intervals with the original source or with the data subject?
>
> Is the fact that the personal data is out of date likely to prejudice the 'policing purpose' or cause damage or distress to the data subject?

5.3 Review, Retention and Disposal

5.3.1 Fifth Principle

The fifth principle of the Act requires that personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes[35]. As with the third principle no interpretative provisions appear in the Act.

The fifth principle requires the police to consider the purpose for which personal data is being held and once that purpose has been concluded the police will either cease processing the personal data (usually through its secure disposal, deletion or destruction), or will de-personalise it in such a way that it is no longer personal data or able to be 'reformed' into personal data.

The police are likely, for practical purposes, to follow the former rather than the latter and adopt a policy of regular review of personal data to establish whether it is still required and dispose as necessary, following the broad approach described in Section 7 of the MoPI Guidance.

Within police forces a systematic approach will be followed including the definition of review periods for particular categories of documents or information containing personal data. At the end of such periods they will be reviewed and disposed of if no longer required.

---

[35] Section 4.6 of the MoPI Statutory Code of Practice includes related provisions

Police forces may need to consider certain statutory requirements which may specify required retention periods, or the potential value of some personal data and other information which may suggest further retention for historic purposes.[36]

ACPO has introduced review and retention periods for information as part of the ACPO Freedom of Information project predating the MoPI Guidance. In addition, case law in 2005 has led to the development by ACPO of 'Retention Guidelines for Nominal Records on the Police National Computer, incorporating the Step Down Model'.

On a practical level within police forces information system owners must ensure that review and 'disposal where necessary' procedures are adopted for systems within their control which apply to both computer and manually-held personal data[37]. However, information system owners must exercise care, particularly with regards to personal data held on computer equipment, to ensure that disposal does mean permanent and complete deletion and that there is no risk of the personal data being 'reformed' or retrieved.

Whatever standard periods are adopted, police forces must maintain a flexible approach towards retention issues which allow individual cases to be assessed properly and proportionate decisions reached regarding retention. This can be achieved through the adoption of exceptional case review procedures and through chief officers, in their capacity as 'data controllers', retaining the right and responsibility to make individual judgements where appropriate.

Exemptions are available from the fifth principle and are summarised found at appendix b.

5.4 Disputes and Complaints

Police forces will develop processes to resolve data quality disputes or complaints regarding the retention or otherwise of personal data.

5.5 Checklist

The following is provided as a brief aide-memoir when considering data quality, review, retention and disposal issues.

Data Quality, Review, Retention and Disposal
What is the specific purpose(s) of the processing?
How is the personal data relevant for that purpose(s)?
How is the personal data not excessive for the purpose(s)?
How is the personal data adequate for that purpose(s)?
How is the personal data sufficient for the purpose(s)?
How is the personal data accurate?
Where necessary, how is the personal data kept up-to-date?
How will a review of the continued retention of the personal data be undertaken?
When will the purpose been achieved?
Is there a requirement in law to retain the personal data?
Is the personal data of historic value?
Is the deletion/disposal permanent and secure?

[36] See DPA section 33 exemption.

[37] Such retention periods would form part of data protection operating rules – see 8.6

5.6 Standards

Standard	Source
Police force has adopted measures to ensure that any personal data processed is adequate, relevant, not excessive, accurate, and kept up-to-date.	5.2
Police force has adopted procedures to ensure that personal data is reviewed and disposed, retained, de-personalised, when no longer required.	5.3.1
Police force has established a process to resolve data quality disputes/complaints.	5.4

6 Subject Access

6.1 Overview

This chapter provides a summary of the right of 'subject access' and describes the procedures which police forces should adopt to ensure that the right is managed in a consistent and proper way.

The following pages describe a framework procedure for processing subject access applications and introduce the standard subject access application form. They also explain criteria for determining an 'acceptable' application, the circumstances in which information and personal data may be withheld (including the most commonly used exemptions), responding to applicants and various other considerations.

Other rights are covered in chapter 6.

6.2 Right of Subject Access

The sixth principle of the Act states that personal data shall be processed in accordance with the rights of data subjects. Subject to exemptions, sections 7-9a[38] of the Act provide individuals with a right of access to their personal data – a process known as 'subject access'.

Upon making a request in writing (which includes transmission by electronic means), and upon paying the required fee to the police force and having proven their identity an individual is entitled:

To be told by the police force whether it or someone else on their behalf is processing that individual's personal data.

If so, to be given a description of:

a) the personal data,
b) the purposes for which they are being processed, and
c) those to whom they are or may be disclosed.

To be told, in an intelligible manner, of:

a) all the information, which forms any such personal data. This information must be supplied in permanent form by way of a copy, except where the supply of such a copy is not possible or would involve disproportionate effort or the individual agrees otherwise. If any of the information in the copy is not intelligible without explanation, the individual will be given an explanation of that information, e.g. where the data controller holds the information in coded form which cannot be understood without the key to the code, and

b) any information as to the source of those data. However, in some instances the data controller is not obliged to disclose such information where the source of the data is, or can be identified as, an individual.

Subject access is a statutory right that police forces must accommodate. However, it should not be seen as an alternative or a replacement for routine disclosures or good business practice. Police forces may engage with individuals to ensure that their problems are resolved rather than forcing them into the 'subject access route'.

Although personal data often forms part of a document, it is important to recognise that the right is one of access to the personal data, and not necessarily to document.

[38] DPA section 9 is unlikely to be of relevance to forces. Schedule 1 part 2 paragraph 8 contains further interpretation of the sixth principle.

6.3 Subject Access Procedure

Police forces will adopt arrangements which will ensure that:

The standard subject access application form (see 6.4) is freely available to enquirers/applicants;

Where the application is unsatisfactory that fact is communicated to the applicant in a timely manner (see 6.6);

'National' subject access applications are forwarded without to the National Identification Service (NIS), while 'local' applications are handled in force (see 6.5);

'Local' subject access applications are forwarded to appropriate staff to acknowledge, assess their 'acceptability', and process without any unnecessary delay (see 6.6);

Where a 'local' application is accepted as satisfactory, a search is initiated of police force electronic records, filling systems and databases that might contain the applicant's personal data;

Any personal data produced from that search, relating to the applicant, is scrutinised by relevant staff (normally by the information system owner, data protection officer and others as necessary). That scrutiny is necessary to confirm the purpose(s) of the processing and to consider the factors described under 6.7 which are designed to ensure that only appropriate personal data is disclosed to the applicant - the information will be edited or redacted as necessary.

Other considerations (see 6.8) are also taken into account;

The personal data which the applicant is entitled to receive is provided to them within the forty calendar day statutory timescale, with consideration of the appropriate wording to be employed where some personal data is withheld (see 6.9);

Force records are updated where appropriate (see 6.11 and 6.12);

Any enquiries or complaints arising from or relating to the application process are dealt with in an appropriate manner (see 6.13);

Information generated by subject access applications is only retained as long as is necessary (see 6.14).

6.4 ACPO Standard Application Form

Applications for personal data under subject access must be made in writing. Standard forms provide benefits to both police forces and to applicants (although police forces cannot insist on their completion). A standard subject access application form has therefore been devised and police forces will base their own forms on the template that can be found at the end of this chapter.

The form has been designed to facilitate the right to be informed that the applicant's personal data is being processed (section 7(1)(a)) and to be provided with a copy of that personal data (section 7(1)(b)(i) and section 7(1)(c)(i)).

Police forces may chose to make their subject access application forms available at police premises across the police force area and on the internet.

Police forces will consider having various alternative routes available to applicants when submitting their applications to the police force e.g. via post, via appointment, via internal post following delivery to their operational police premises, or electronically[39].

[39] Electronic means should only be adopted where forces have also developed appropriate measures to also confirm the

Applicants will be encouraged to apply to the police force in whose area they reside or most recently resided where they seek access to nationally-held personal data. Requests for personal data held or processed by a particular police force will be directed to that police force.

6.5 'National' and 'Local' Applications

Subject access applications to arrest, prosecution, conviction, caution, reprimand & warning information, existence of firearms, shotgun and explosive licences, held on the Police National Computer (PNC) are referred to as 'national' applications. These are distinguished from subject access applications to all other information held locally by police forces – the latter are known as 'local' applications.

'National' applications will be forwarded to the National Identification Service (NIS), who will process them in accordance with the ACPO-NIS Service Level Agreement[40] and associated 'Editing Guidance'.

Note: By the summer of 2009 the NIS will cease to handle 'National' applications on behalf of police forces. That service will be taken over by ACPO's Criminal Records Office (ACRO). It is anticipated that initially ACRO will replicate the well-established procedures available through ACRO. Future versions of this manual will be adapted to reflect any changes that the transfer of service may lead to.

The remaining 'local' applications will continue to be handled within the police force itself.

A single subject access application that seeks access to both 'national' and 'local' information will be split accordingly, though only one fee may be charged.

6.6 'Satisfactory' Applications

Any subject access application will be initially assessed to ensure that it is acceptable with regard to the aspects described in the remainder of 5.6. If the application is unsatisfactory the applicant must be advised accordingly. However, in any case all applications should be forwarded to appropriate staff, acknowledged and processed without any unnecessary delay.

6.6.1 Fee

Police forces may charge the standard fee, subject to the statutory maximum (£10 as of 31st August 2006). A fee of up to £10 may be charged where a single application is made to both nationally-held personal data, and other personal data held locally by police forces (see 6.5). If the required fee is not forthcoming the application may be rejected.

6.6.2 Identification

It is important to confirm the identity of the person making the application to ensure the personal data is disclosed to the data subject and not someone impersonating them.

Police forces will, **as a minimum**, request copies[41] of at least two different official documents which between them provide sufficient information to prove the applicant's name, date of birth, current address and signature[42]. For example:

---

applicant's identity and obtain payment.

[40] Generally, police forces are unable to 'chase up' national applications prior to 'due date' - applications are dealt with by NIS on a strictly 'first come first serve' basis, and no priority can be assigned to individual applications. If an applicant's 'due date' is reached and they have not received a reply from ACRO they should contact the police force no later than 14 days after the 'due date' in order that the force can communicate with ACRO on their behalf. ACRO are not in a position to issue a reply after that additional 14 day period has passed (i.e. 54 days from the date the application was accepted by the police force) - in such circumstances applicants will need to restart the whole application process.

[41] Police forces who choose to accept copies of documents, rather than the original documents themselves, may wish to consider the following: a) HMSO Guidance Note on the reproduction of the British Passport; and b) HMSO Guidance Note, relating to the copying of Birth, Death and Marriage Certificates.

[42] In some exceptional circumstances the applicant may already been sufficiently known to the police force so there may be no

A combination of driving licence, medical card, birth/adoption certificate, passport, and any other official documents which show name, date of birth, address and signature.

Police forces may require further information to satisfy themselves as to the identity of the applicant and will inform the applicant of that requirement where necessary.

Police forces may also wish to include a disclaimer on correspondence with applicants advising them that the police force will not be held accountable for any identity documents lost in the post. Police forces may agree to return identity documents by recorded delivery where the applicant has made all the necessary arrangements and payments.

Applicants not wishing to post their identification documents may be offered the alternative of attending one or more of the force's police stations to display those documents.

The signature of the applicant will also be required to assist in the identification process.

6.6.3 Sufficient Information

If an application does not provide sufficient information as is 'reasonably required' by the police force to locate the personal data sought, the police force must inform the applicant that further information is required. These steps must be taken as soon as possible after receiving an application and will guide the applicant as to what further information is needed to satisfy the requirement.

Police forces must decide what is 'reasonable' as a minimum requirement. It may be useful for the applicant to answer questions such as:

Why do they believe their personal data is being processed?

Under what circumstance did they have contact with the police?

When and where was that contact?

In most circumstances, a subject access application 'for everything you hold about me' would in itself constitute insufficient information. However, there may be limited occasions where the nature of the relationship between the applicant and the police force and context of the request could make such a request sufficient.

In cases where the application is one that will be forwarded to the NIS there will not normally be a requirement for further information to be provided by the applicant other than those details required by the police force's subject access application form.

Where the application is for unstructured personal data (as per the definition under section 1(1)(e) of the Act) the application must include a description of the data[43].

6.6.4 Applications made on behalf of another – Agents/Power of Attorney/Persons with Disabilities

Police forces may receive subject access applications by agents or others acting on behalf of an individual who is unable to make the application themselves – for example, solicitors or those granted the power of attorney, or partners of those with disabilities.

In such circumstances the police force may be provided with suitable written evidence to confirm that

---

need for such measures to be employed – for example, a current employee (in such circumstances there is also likely to be no requirement to record the height of the applicant).

[43] Requirement derived from DPA section 9A (an amendment created by the FOI Act). Section 9A also introduces a cost related exemption – see 6.7.3.2

the person has the power to act on behalf of the data subject.

6.6.5 Applications made on behalf of another – Young Person

Subject access applications can be accepted from a young person where they are believed to have sufficient intellectual ability to understand the nature of the application.

It is generally presumed that a person of twelve years of age or more will have sufficient age and maturity to exercise the right of subject access[44]. In other cases a child under that age will still be able to exercise the right where they have a sufficient general understanding of what it involves.

A parent or guardian can exercise the right and receive the reply, if the young person does not have the intellectual ability to understand the nature of the application, and the parent is though to be acting in the best interests of the young person.

Consideration must be given to requesting the young person's birth or adoption certificate or other evidence to show the parent or guardian has the responsibility for him/her.

Caution must be exercised when dealing with such applications where it is clear that the young person's parents are in dispute with one another and the application may not be in the best interests of the young person.

6.6.6 Repeated Applications

Under section 8(3) forces are not obliged to comply with an identical or similar application to one already received from the same applicant unless a 'reasonable interval' has elapsed between the two requests. In deciding what amounts to a 'reasonable interval' the following factors should be considered:

the nature of the personal data;

the purpose for which it is processed;

the frequency with which the personal data is altered.

6.7 Circumstances when information and personal data may be withheld

A combination of provisions covering third-party personal data, disproportionate effort and exemptions, may restrict access to personal data sought under the subject access process. In addition, there may be instances where other statutory obligations further restrict the disclosure of personal data.

Decisions to withhold personal data and other information from 'National' applications will be handled in accordance with the ACPO-NIS Service Level Agreement. For the remaining 'local' applications those decisions rest with the police force.

6.7.1 Third-Party personal data

Police forces may not be obliged to disclose third-party personal data – i.e. personal data relating to someone other than the subject access applicant. This applies to the obligation on police forces to provide details of the source of the personal data held. If the source of the personal data identifies a third-party it can be withheld - a process which is usually achieved by editing or redacting the response.

Under section 7(4)(a) & (b) information about a third-party can only be disclosed if: -

the third-party has given consent to the person making the request; or

it is reasonable to reply to the request without consent of the other individual.

[44] See DPA section 66(2).

In these circumstances, due regard has to be given to a balance of interest of the parties concerned. In deciding this question regard should be had to any duty of confidentiality (see 3.2.2.1) owed to the other individual, any steps taken by the police force with a view to seeking the consent of the other individual, whether the other individual is capable of giving consent, and any express refusal of consent by the other individual.

In most circumstances it will be appropriate to disclose a police officer's name or other identifiers, where he or she is acting in an overt professional capacity.

Specific measures may need to be taken when responding to applications for access to CCTV material. It may be necessary to blur any images of third parties on the material unless they do not have a reasonable expectation of privacy for example, if they are in a public place.

6.7.2 Disproportionate Effort

Under section 8(2) of the Act, personal data found in response to a subject access application does not have to be provided in permanent form to the applicant if the process of creating the permanent copy would involve 'disproportionate effort'.

The Information Commissioner's view is that the disproportionate effort does not relate to the difficulty or workload that may be encountered in retrieving the personal data in the first place prior to providing it to the applicant.

The following is likely to be a case where 'disproportionate effort' was applicable:

> *The applicant's personal data is contained on a very old stand-alone computer system. The system is such the information can only be viewed on screen and cannot be exported or printed.*

Where disproportionate effort is appropriately claimed, the police force will be required to look for alternative means to supply access to the personal data.

The following factors will be considered as part of any deliberations on disproportionate effort:

What information/assistance has the applicant provided in identifying the personal data;

What a reasonable person would believe to be a reasonable amount of effort – bearing in mind the £10 fee;

How much extraction/redaction time is needed, depending on the complexity of the information and the manner in which is stored;

Where the individual has not specified that they want the information, what is the impact on the individual of not having the information compared to the amount of effort in providing it.

Any police force intending to use the disproportionate effort clause is recommended to contact the ACPO Data Protection Portfolio Secretary for further advice.

6.7.3 Subject Access Exemptions

There are a number of exemptions within the Act that recognise that there may be a public interest in withholding personal data sought under subject access. The remainder of this section (up to 5.7.4) covers the ones most likely to be employed by the police. It therefore should be read in conjunction with 5.9 which explains the wording to be provided to applicants when exemptions are used.

Exemptions must not be used as a 'blanket' to withhold everything the police holds on an applicant. They will be used on a case-by-case basis and only to the extent required.

6.7.3.1 Section 29(1): Crime and Taxation

This allows the police to withhold personal data sought under subject access where disclosure would be likely to prejudice the prevention or detection of crime, apprehension or prosecution of offenders, or the assessment or collection of any tax or duty of any imposition of a similar nature.[45]
Personal data likely to fall under this exemption will be found in the records and information holdings of all 'operational' elements of a force, including special branch, basic command units, intelligence units, criminal justice and major investigations departments. In addition, it may be relevant to some 'non-operational' departments.

The following are provided as examples where section 29(1) may be used:

Application from a suspect seeking access to personal data held on intelligence systems in order to determine the level and nature of police interest in, or intelligence held on, him/her;

Application from a defendant in a forthcoming trial seeking access to personal data associated with those ongoing proceedings;

Application for access to personal data which if disclosed was likely to diminish future assistance to the police by the public;

Application for access to personal data whose disclosure would reveal confidential police techniques.

Where a police force determines that the section 29(1) exemption is applicable the police force will respond to the applicant in accordance with 5.9.

In cases where the personal data had already been officially released to the applicant through disclosure under the Criminal Procedures and Investigations Act 1996 it is unlikely that the exemption would apply.

6.7.3.2 Section 9A: Appropriate Fees Limit (Unstructured personal data)

Section 9A provides an exemption relating to unstructured personal data where the estimated cost of complying with section 7(1) would exceed the appropriate fee limit – currently £450 or 18 person/working or equivalent-hours - derived from The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004 which were made under section 12(5) of the Freedom of Information Act 2000.

The exemption does not cover the need to inform the applicant whether their personal data is being processed unless to do so alone would exceed the appropriate fees limit.

Police forces intent on using this exemption will consider documenting any calculations and rationale used in case of challenge.

The following is provided as an example where section 9(A) would be likely to be utilised:

Application seeking access to personal data held in a large unstructured crime file dating from the 1960s where the appropriate fee limit was likely to be breached.

6.7.3.3 Section 28(1): National Security

This primary exemption allows the police to withhold personal data sought under subject access where non-disclosure is necessary 'for the purpose of safeguarding national security'. It should be noted that the section 28 exemption is not restricted simply to non-disclosure under subject access, but is

[45] The case of R (Lord) v Secretary of State for the Home Department [2003] EWHC 2073 (Admin) provides useful guidance on the meaning of likely to prejudice.

applicable more generally to most of the Act where necessary to protect processing for national security purposes.

Although the term 'national security' is not defined within the Act, section 1 of the Security Service Act 1989 (as amended by the Security Services Act 1996) describes the broad function of the Security Service ('the protection of national security') and 'in particular, the protection against threats from espionage, terrorism[46] and sabotage, from the activities of agents of foreign powers and from actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means. It shall also be the function of the [Security] Service to safeguard the economic well-being of the United Kingdom against threats posed by the actions or intentions of persons outside the British Islands'; and 'to act in support of the activities of police forces and other law enforcement agencies in the prevention and detection of serious crime'. These extracts may provide useful pointers to help police forces determine what constitutes 'national security'.

Where a police force decides that the use of section 28(1) is appropriate then in most cases it is likely that the section 29(1) exemption will also be applicable. Police forces may be content to rely solely on the section 29(1) exemption is such circumstances.

Section 28(2) provides that a certificate signed by a Minister of the Crown certifying that the use of the section 28(1) exemption is, or at any time was, required for the purpose of safeguarding national security shall be conclusive evidence of that fact. It is not necessary to have a certificate in order to rely on the section 28(1) exemption but it will strengthen the position of the police force in any legal proceedings, and determine the forum for hearing an appeal. When a ministerial certificate has been served, any appeal is heard by the National Security Appeals Panel of the Information Tribunal rather than by the Information Commissioner.

Personal data relating to national security matters is most likely to be held by police forces' special branch, executive, intelligence, contingency planning, criminal justice and major investigations departments. Of course, such material may permeate in various forms into other areas of the police force. It does not follow, however, that all information within those departments relates to national security matters.

The police are likely to hold information, including personal data, relating to national security matters in a number of classes including:

Information obtained from 'the agencies' - Security Service ('MI5'), the Secret Intelligence Service (SIS or 'MI6'), the Government Communications Headquarters (GCHQ) - and the Serious Organised Crime Agency (SOCA) and Government Departments including the armed services;

Information obtained, created or developed by the police in response to the receipt of the above information;

Information obtained, created or developed by the police in order that it can be provided to 'the agencies', SOCA and Government Departments;

Information relating to the 'agencies', SOCA and Government Departments.

Ordinarily most personal data in those classes will be of such a character that confirming its existence or disclosing it under subject access (or other means) would risk adverse repercussions to the operational effectiveness of the police and other agencies' safeguarding of national security functions.

It is recognised that the time period during which prejudice to national security will occur (through the disclosure of such personal data) is likely to be significantly longer than that arising from the related prejudice to 'policing purposes'.

The following are provided as examples where the non-disclosure exemption within section 28(1) may

[46] 'Terrorism' is itself defined in section 1 of the Terrorism Act 2000.

be used:

Application from a terrorist suspect or associate seeking access to personal data held on intelligence systems in order to determine the level and nature of police interest in, or intelligence held on, him/her;

Application from a member of the police who had failed national security vetting on the basis of intelligence and was using subject access as a means to find out why;

Application for access to personal data whose disclosure would reveal confidential police or agency techniques, such as those relating to intercepts.

When considering the applicability of section 28(1) police forces should be mindful of the following:

In cases where it has been officially admitted (for example, in court) that the applicant's personal data is being processed to safeguard national security then it is unlikely that section 28(1) could be used to deny that personal data is being processed – however, in all but exceptional cases section 28(1) would still be used to withhold the personal data itself.

But, in view of the very nature of this exemption, police forces are likely to take a precautionary approach that will tend to result in non-disclosure on 'borderline' cases. This stance has been accepted in prior case law.

Where a police force identifies that section 28(1) may be applicable to a subject access application, it will adopt the following procedure:

At the earliest opportunity the data protection officer will contact with the ACPO Data Protection Portfolio Secretary ('the Secretary') to advise of the receipt of the application and the likelihood that section 28(1) applied.

The Secretary will provide further guidance as to how the application should proceed in accordance with ACPO-agreed guidelines.

Where it is deemed that section 28(1) is applicable, a formal endorsement of its use will be made by staff within the police force at an appropriate level. This may involve the submission of a report to the chief officer with responsibility for data protection matters, specifying the adverse repercussions if the exemption was not used, including any advice received from the secretary, and seeking approval for the response to the applicant.

Where the chief officer agrees that the section 28(1) exemption is applicable the police force will respond to the applicant in accordance with 5.9.

In the event of any appeal to the disclosure decision, the ACPO Secretary must be informed immediately to issue further guidance.

Throughout the above procedure personal data should only be processed where absolutely necessary – in most cases it is anticipated that a particular case will be discussed in its generality without the need to identify data subjects.

6.7.3.4 Section 30: Health, Education & Social Work

This exemption provides powers for the Lord Chancellor to make orders providing exemptions in relation to health, education and social work records. Orders relating to all three categories of records have been made.

Where the application is for personal data relating to the applicant's physical or mental health, an exemption within The Data Protection (Subject Access Modification) (Health) Order 2000 allows the withholding of the personal data sought under subject access – provided it was considered that the disclosure was likely to cause serious harm to the physical or mental health of the applicant or another

individual.

The following is provided as an example where this provision may be considered by the police:

Application seeking access to sensitive personal data held by a police force's occupational health or welfare department.

Before deciding as to whether this exemption applies the police force is obliged [by Article 5(1) and 6(1) of the Order] to consult the health professional responsible for the clinical care of the applicant or, if there is more than one, the most suitable available health professional (health professional is defined under section 69 of the Act). There is no need to consult where the applicant already knows about the information [Article 6(1)], nor in limited circumstances where the consultation has already been carried out prior to the request being made [Articles 7(1) and (2)].

A further exemption is conferred in certain circumstances where a third-party is making the request on behalf of the applicant, and the applicant does not wish that information to be disclosed to the third-party [article 5(3)].

In view of the sensitivity of personal data relating to an applicant's health, police forces may wish to ensure that it is disclosed directly from the health professional to the applicant. Alternatively it could be given to those handling the subject access application in a sealed envelope for onward transmission to the applicant.

6.7.3.5 Section 33A(2): Manual Data held by public authorities

This covers 'category e' personal data where it is held for personnel purposes. The following is provided as an example where this provision may be considered by the police:

To withhold personal data held within a personnel file that consisted of unstructured manual data.

6.7.3.6 Schedule 7: Miscellaneous Exemptions

The following are likely to be the exemptions under Schedule 7 most relevant to the police:

Paragraph 1: Covers confidential references given by the police force in relation to education, employment or the provision of services. (It does not cover references supplied to the police force, though in such cases the duty of confidentiality to the supplier of the reference should be considered). The following is provided as an example where this provision may be considered by the police:

To withhold a confidential reference about a police force employee supplied to another organisation sought under subject access to the police force providing the reference.

Paragraph 7: Covers personal data consisting of records of the data controller's intentions in relation to negotiations with the data subject. The exemption may be applied to:

Withhold confidential personal data sought under subject access that had been prepared in relation to a forthcoming redundancy offer to the applicant.

Paragraph 10: Covers personal data in respect of which legal professional privilege could be claimed. Legal opinion provided by the CPS may not be covered by this exemption. The exemption may be used to:

Withhold personal data contained in legal advice to the chief officer from the police force solicitor. The information would also be likely to be protected by legal professional privilege.

Police forces must use care when applying exemptions and will document in their own records which exemptions have been used for subsequent scrutiny, as required. In some exceptional cases police

forces may choose to use their discretion and not employ an exemption which they could have used.

A summary of the exemptions from subject access and other elements of the Act can be found in appendix b.

6.7.4 Information other than Personal Data or Third-Party Personal Data

In most cases when a police force retrieves personal data for disclosure to a subject access applicant that personal data will be surrounded by other information which will not be the applicant's or another's personal data. For pragmatic reasons this 'other information' may be disclosed to the applicant, though police forces must recognise that this represents a provision of information beyond that required by the Act.

6.8 Other considerations

6.8.1 Routine Amendment and Deliberate Destruction

Under section 8(6) the information supplied in response to a subject access application must reflect the personal data held at the time the application was accepted by the police force. However, account may be taken of any routine amendment or deletion made between receiving and responding to an application, provided that it had not been made as a result of receiving the application.

Under section 77 of the Freedom of Information Act 2000 it is an offence for a police force to alter, deface, block, erase, destroy or conceal information and personal data sought under the subject access and Freedom of Information Act processes if it is done with the intention of preventing the disclosure of all or part of the information and personal data sought.

6.8.2 Personal Data in a Force's possession which was derived from another body

Police forces are obliged to consider all personal data in their possession when they receive a subject access application, irrespective of where that personal data originated from. Some applications are likely to encompass information which was provided by or created by third-party organisations or individuals (i.e. not the police force or the applicant). Examples would include:

> *Personal data contained in documents created by other police forces, doctors, solicitors, the Crown Prosecution Service etc.*

In such cases, and where practical, the police force may choose to write to the provider of the information to explain that an application had been received and ask formally for their views on disclosure of any personal data to the applicant – on the basis that the provider would be in a position to comment on exemptions relevant from their perspective. The correspondence could indicate that unless an objection was received before the end of the forty-day deadline the police force may disclose the personal data sought.

In all cases, irrespective of the provider's comments, the final decision on disclosure rests with the police force receiving the subject access application.

The following is an example of such a scenario:

> *The police force receives a subject access application for personal data relating to a victim or suspect in a recent joint police-social services investigation. Some of the information held by the police comprises of reports provided to the police by social services. The police could consult with social services regarding the application of exemptions from their perspective.*

> *The police force receives a subject access application for personal data obtained from the Security Service (see 6.7.3.3)*

6.8.3 Hybrid FOI-Subject Access applications

Police forces are likely to receive single requests for both recorded information and personal data relating to the applicant under the statutory provisions of the Freedom of Information and Data Protection Acts. On such occasions they are recommended to co-ordinate the request under both Acts.

6.8.4 'Accelerating' applications

Police forces are likely to receive requests from applicants to 'accelerate' their applications, particularly those that will be handled by the National Identification Service.

Police forces must not to attempt to prioritise in that manner except in wholly exceptional circumstances – such as where the application is urgently sought to allow an overseas visit to a dying relative.

6.9 Responding to applications

Once an acceptable application has been received and processed, police forces must reply to the applicant promptly and in any event within forty calendar days, even if personal data is not held or an exemption is relied upon.

Any personal data provided must be in permanent form, and be legible to the applicant. If it cannot be fully transcribed into an intelligible format an explanation will be given of any code used in the response.

Subject access is a right to the personal data, rather than to documents themselves, and in some cases the most appropriate means of providing personal data will be to extract or copy it from the source document into the response.

Generally, responses to applicants will be one of the following:

1. Full disclosure - in cases where the police force has determined that all the applicant's personal data will be disclosed, the applicant will be advised along the lines that:

"The Data Protection Act places an obligation on the chief officer, when holding personal data, to provide a copy of that information, (unless an exemption applies), to you on request. From the personal details supplied in your application, please find enclosed the information that the chief officer is required to supply to you under the provisions of the Act."

2. Partial-disclosure - in cases where the police force has determined to withhold, via the use of exemptions, some of the applicant's personal data, the applicant will again be informed along the lines that:

"The Data Protection Act places an obligation on the chief officer, when holding personal data, to provide a copy of that information, (unless an exemption applies), to you on request. From the personal details supplied in your application, please find enclosed the information that the chief officer is required to supply to you under the provisions of the Act."[47]

3. Non-disclosure - in cases where the police force has determined to withhold, via the use of exemptions, all of the applicant's personal data, the applicant will be informed along the lines that:

"The Data Protection Act places an obligation on the chief officer, when holding personal data, to provide a

[47]All police forces are recommended not to reveal the use of an exemption to the applicant. However, the rationale behind the use of the exemption must be recorded by the police force for reference in any subsequent appeals process (both internal and via the Information Commissioner). The non identification of the exemption to the applicant is suggested because: (i) there is no legal requirement to do so; (ii) in a particular case, the mention of the use of the exemption would negate the effectiveness of that exemption; and (iii) generally, a consistent approach should be adopted across the police service.

copy of that information, (unless an exemption applies), to you on request. From the personal details supplied in your application, there is no information that the chief officer is required to supply to you under the provisions of the Act."[48]

4. Nothing held - in cases where no personal data is processed the applicant will be given the reply along the lines that:

"The Data Protection Act places an obligation on the chief officer, when holding personal data, to provide a copy of that information, (unless an exemption applies), to you on request. From the personal details supplied in your application, there is no information that the chief officer is required to supply to you under the provisions of the Act."

All responses will normally be sent directly to the applicant at their home address. However, there may be occasions when the applicant specifically requests that nothing be sent to their home address. Such requests must be made in writing by the data subject. In these circumstances the response may be either sent to an alternative address nominated by the applicant or arrangements can be made so that the applicant attends police premises to collect the response in person. In the latter scenario a police force will need to be satisfied as to the person's identity.

In the unlikely event that the forty-day statutory period will not be met, it is recommended that police forces contact the applicant to warn them of the delay.

6.10 Enforced Subject Access

Certain employers, loss adjusters and foreign governments exploit the subject access process by requiring individuals to use it to obtain a copy of their criminal convictions on PNC (or evidence that there is nothing held) as part of recruitment/employment, insurance claim or emigration processes.

Although this is not currently illegal under the Act, it may be interpreted as contrary to the spirit of the Rehabilitation of Offenders Act 1974 as in some cases it forces those individuals to reveal 'spent' offences that they would not have to disclose if the provisions of the Rehabilitation of Offenders Act 1974 were applied.

In due course this will become an offence once section 56 of the Act is enacted. That section makes it an offence for a third-party to require an individual to use subject access where the information sought is required by the third-party in connection with employment purposes or the provision of services, and where the information would reveal prior conviction or caution details. Section 56 will not have effect until the 'Basic Disclosure'[49] becomes available from the Criminal Records Bureau (CRB).

Although the CRB's 'Basic Disclosure' is currently unavailable, equivalent checks have been introduced by The Scottish Criminal Record Office Disclosure Service, commonly known as 'Disclosure Scotland', and by Access Northern Ireland. Police forces are encouraged to advise subject access applicants of the existence of those services where those applicants express a concern that the subject access process would require them to reveal 'spent' convictions and their applications are related to employment purposes.

6.11 Criminal Procedure & Investigations Act 1996 (CPIA)

Where a subject access application results in the disclosure of copies of intelligence, crime files, or prosecution files, police forces should consider the desirability of ensuring that a record of, or reference to, that disclosure is available within the original documentation. This may assist in alerting staff to the fact that a disclosure had been made and thus assist compliance with the requirements of the CPIA.

---

[48] See previous footnote.

[49] A 'basic disclosure' contains details of convictions considered unspent under the Rehabilitation of Offenders Act 1974.

6.12 Updating Records from Subject Access applications

Where police forces receive subject access applications from persons of interest to them for 'policing purposes', they will consider, on a case-by-case basis, using information contained in the application to update or augment existing records or to create new records in accordance with national standards.

6.13 Formal withdrawal of Subject Access applications

In some instances applicants may decide that they wish to withdraw a subject access application after it has been accepted by a police force. In such instances police forces are encouraged to obtain confirmation of the withdrawal in writing.

6.14 Appeals/Complaints Process

Police forces will establish a process to handle appeals or complaints by applicants dissatisfied with the response to their subject access application. The process may take the form of an internal review procedure, followed by referral to the Information Commissioner (similar to that adopted by the police under the FOI Act); or simply, a response to the applicant suggesting that they contact the Information Commissioner in the first instance.

6.15 Review and Retention of Subject Access Application Information by Police Forces

6.15.1 'National' (NIS) Applications

Police forces will adopt a standard retention period of two years for summary details of 'National' (i.e. those sent to the National Identification Service) subject access applications. At the conclusion of the two-year period the continued retention of that information will be reviewed, and where it is no longer justified the information will be destroyed. Those police forces that choose to send copies of application forms to NIS will assess the need for retention of the original application form after two years. Application forms sent to NIS by police forces will be retained by NIS in accordance with the ACPO-NIS Service Level Agreement.

6.15.2 'Local' Applications

Police forces will adopt a standard retention period of two years for all information related to 'local' subject access applications. At the conclusion of the two-year period the continued retention will be reviewed, and where it is no longer justified the information will be destroyed.

Police forces will attempt to distinguish between 'routine' subject access applications and others where the circumstances may suggest a longer retention would be prudent. Factors to consider in such a judgement include:

whether the force's handling of the application has been, or is likely to be, subject to complaint;

whether it is high 'high-profile' in nature;

whether the application involved the use of 'unusual' exemptions.

6.16 Standards

Standard	Source
The ACPO standard subject access application form is freely available to enquirers/applicants.	6.4
Police force handles 'National' applications in accord with the ACPO-NIS SLA.	6.5
Police force has adequate procedures in place to inform subject access applicants with 'unsatisfactory' applications of that fact in a timely. manner.	6.6
Police force has adequate procedures in place to handle 'local' subject access	6.6-6.9

applications.	
Police force has adequate procedures for ensuring that CPIA requirements are satisfied where required.	6.11
Police force has sound procedures to update or augment existing records, or create new records, with information obtained from subject access applications.	6.12
Police force has established a subject access appeals/complaints process.	6.13
Police force has robust procedures in place to ensure subject access application information is retained only as long as necessary.	6.14

Form SA1: Application for access to your personal data held on Constabularyshire Police information systems

Section 7(1)(a) & 7(1)(b)(i) & 7(1)(c)(i) of the Data Protection Act 1998 (Subject Access)

Your Subject Access Rights
Subject to certain exemptions, you have a right to be told whether Constabulary Police holds any information about you (your 'personal data') and a right to be provided with a copy of that personal data within a 40 day period.

If you wish to exercise those rights please complete this form carefully and follow the instructions regarding the £10 fee, proof of identity, and ways to return the form to Constabulary Police.

The Data Protection Act means that in certain circumstances Constabulary Police may decide not to provide you with some personal data. For example, we will not provide personal data if we feel releasing it to you would be likely to prejudice policing purposes, and we may not provide you with information that identifies other individuals.

Fee
Your Subject Access application will cost £10. You are encouraged to pay by cheque as regulations over the handling of cash may delay your application. Cheques etc. should be made payable to 'Constabularyshire Police'. Postal Orders must be UK Postal Orders.

Proof of identity
Constabulary Police needs to be satisfied that you are who you say you are. Consequently Section 3 asks you to provide evidence of your identity and address by supplying copies of at least two official documents which between them provide sufficient information to prove your name, date of birth, current address and signature.

Returning this form
The completed form, with appropriate fee, proof of identity, date of birth and address documents should be returned to Constabularyshire Police using any of the following methods:

[enter options here]

Section 1. About Yourself *(Please use block capitals and black ink)*

Surname/Family Name ..... Title (Mr/Mrs etc) .....

First/Fore Name(s) .....

Former/Maiden Name(s) ..... Height .....

Sex/Gender (Male/Female) ..... Date of Birth .....

Place of Birth (Town & County/Country) ....

Home Address .....
This is the address to which all replies will be sent, unless you specify otherwise below .....

..... Postcode .....

Daytime Telephone Number(s)* Work..... Home .....

Email Address(es)* Work..... Home .....

** Not mandatory, but these will assist us if we need to get back in touch with you to discuss your application.*

Alternative Delivery Address .....
Only complete this if you wish us to send our reply to an address different to your current address .....
You will need to provide us with Evidence of your connection with this address. .....

The information supplied in connection with this application will be used for the purpose of administering this request and to ensure the accuracy of Police systems.

Previous Addresses
If you have lived at the above address(es) for less than ten years please give your previous addresses for that period in the box to the right. Continue on a separate sheet if you need to

Section 2. Personal Data Sought

☐ Tick here if you wish to access details of your 'Person Record' on the Police National Computer. This may include details including Arrests, Prosecutions, Convictions, Cautions, Reprimands & Warnings, Firearms, Shotguns and Explosives Certificate Holders and other details. *Not all arrests, prosecutions, convictions, cautions, reprimands and warnings are held on the PNC.*

☐ Tick here if you wish to access personal data other than the above. To help us find any information that may be held about you, please supply additional details in the box below (and continue on a separate sheet if you need to). *To assist us you are advised to include, where relevant: a description of the information you are looking for; a crime reference or incident number; a description of the circumstances in which you had contact with the Police – for example were you a person reporting an offence or incident, a witness, a victim, a correspondent, an offender etc?; dates and times; and any other information you have that can assist us in finding the information you seek.. If you are requesting photographs or CCTV footage please supply a photograph of your face (e.g. passport photo) to assist identification.* ***Please note a failure to provide such details may result in your application being rejected and returned to you.***

Section 3. Proof of Identity Documents

To help establish your identity your application must be accompanied by copies of at least **two** different official documents which between them provide sufficient information to prove your **name, date of birth, current address & signature**. *For example, a combination of driving licence, medical card, birth/adoption certificate, passport, and any other official documents which show those details.*

Section 4. Declaration (to be signed by the applicant)

The information, which I have supplied in this application, is correct, and I am the person to whom it relates.

Signature..... Date .....

Warning – A person who impersonates another or attempts to impersonate another may be guilty of an offence

Should any advice or guidance be required in completing this application, please contact: The Information Access Officer, Constabularyshire Police, Police HQ, PO Box 1, Anytown AA1 1AA. Tel: 01234 567890 email dataprot@const.pnn.police.uk

To be completed by officer receiving

Check that the form has been completed and is legible and you are satisfied with the applicants' identity. Then complete the form below accordingly. If a cheque or postal order is used for payment forward the cheque and form to the Information Access Officer at Police HQ. If payment is made using cash this should be handled in accordance with standard procedures.

Application checked and legible?	Yes/No	Date application received complete	
Identification documents checked?	Yes/No	Completed by: Rank/Number	
Identity document(s) detail		Name	
Identity document(s) returned?	Yes/No	Stationed at	
Fee paid £		Method of payment	
Receipt Number		Signature	

7 Other Rights and Complaints Resolution

7.1 Overview

The first part of this chapter examines individuals' rights under the Act apart from the right of subject access (which was described in the previous chapter). The remainder outlines some measures that data protection officers are encouraged to adopt to help resolve any information disputes and complaints that may arise.

The sixth data protection principle states that 'personal data shall be processed in accordance with the rights of data subjects under this Act'[50].

Rights exist in relation to the following:

Right to prevent processing likely to cause damage or distress;

Rights in relation to automated decision taking;

Right to take action for compensation if the individual suffers damage by any contravention of the Act by data controllers;

Right to take action to rectify, block, erase or destroy inaccurate data;

Right to request the Information Commissioner to assess a data controller's processing.

When handling applications under these rights police forces must be aware of the approach to handing applications made on behalf of another person with respect to the right of subject access (see 6.6.4 and 6.6.5).

A summary of the available exemptions from these rights can be found in appendix b.

7.2 Right to Prevent Processing Likely to Cause Damage or Distress (Section 10)

An individual is entitled to write to a police force requiring that it does not process their personal data in a manner that is causing or is likely to cause unwarranted substantial damage or substantial distress to themselves or another person.

However, certain exemptions apply and section 10(2)(a) is specifically relevant to police information as this right to prevent processing does not apply 'in a case where any of the conditions in paragraphs 1 to 4 of schedule 2 is met'. Paragraph 3 of schedule 2 'The processing is necessary for compliance with any legal obligation to which the data controller is subject…' clearly applies to policing information which is still required in order to allow chief officers to carry out their statutory obligations as defined in the Police Acts, PACE and other pieces of legislation and common law.

All such requests, known as 'data subject notices', will be forwarded as soon as possible upon receipt to the data protection officer to co-ordinate the response. It is important to note that the individual can only serve a data subject notice that relates to personal data in respect of which he/she is the data subject.

This right to serve a data subject notice applies whether the individual objects to the processing taking place at all, or whether the objection relates specifically to processing for a particular purpose or in a particular way.

A data subject notice must:

[50] Further interpretive provisions for the sixth principle are contained in schedule 1 part 2 paragraph 8.

Describe the personal data involved;

Describe the processing to which he/she objects;

State that the processing is causing or is likely to cause substantial damage or substantial distress to him/her or another;

Describe the damage or distress;

State that the damage or distress would be unwarranted;

Give reasons why the processing would cause such distress and would be unwarranted.

The Information Commissioner's legal guidance suggests:

'It is for a court to decide in each case whether the damage or distress is substantial and unwarranted. The Commissioner takes the view that a data subject notice is, therefore, only likely to be appropriate where the particular processing has caused, or is likely to cause, someone to suffer loss or harm, or upset and anguish of a real nature, over and above annoyance level, and without justification.'

Upon receipt of a data subject notice an assessment must be made as to whether or not the data subject notice fulfils the criteria outlined above.

Where it does, consideration must be given as to whether the processing is exempt from the right by virtue of the processing being carried out under any of the grounds under paragraphs 1-4 of schedule 2[51]:

1) the data subject has given a valid consent to the processing (although consent may be withdrawn);

2a) the processing is necessary for the performance of a contract to which the data subject is a party;

2b) the processing is necessary for the taking of steps at the request of the data subject with a view to entering into a contract;

3) the processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract;

4) the processing is necessary to protect the individual's vital interests (i.e. it is a life or death situation).

Where the schedule 2 grounds (paragraphs 5 or 6) are relied upon an assessment will be conducted assessing the police force's legitimate interests in the processing against those of the data subject in order to judge the extent of the damage or distress and to what degree it was unwarranted. This process is likely to involve seeking the views of the information system owner(s) whose systems processed the personal data concerned.

Police forces must reply to a data subject notice within 21 days, having determined whether the notice was warranted and the individual's claims could be substantiated.

That response will indicate whether the police force has, or intends to, agree to the data subject notice, or must state the reasons for regarding the data subject notice as unjustified and the extent (if any) to which the police force has or will comply with the data subject notice.

[51] Derived from DPA section 10(2).

7.3 Right to Prevent Processing for the Purposes of Direct Marketing (Section 11)

Subject to certain exemptions, an individual has the absolute right to request in writing that a police force stops within a reasonable time, or does not start, using their personal data for direct marketing purposes. This includes the communication by any means (e.g. mail, e-mail, telephone, door-to-door canvassing) of any advertising or marketing material directed at particular individuals.

In the unlikely event that such a request is received it will be forwarded as soon as possible upon receipt to the data protection officer to co-ordinate the response.

7.4 Rights in Relation to Automated Decision Taking (Section 12)

Subject to certain exemptions, an individual has the right to require that a police force ensures no decision that would significantly affect them is taken by the police force or on its behalf purely using automated decision-making software. The right has to be exercised in writing.

If there is a human element involved in the decision-making the right does not apply.

Examples of automated decision-making include:

Issuing a court summons to a person recorded as a vehicle keeper with the DVLA on the basis of a safety camera reading without any further investigation or intervention;

Filtering of job applicants using psychometric testing scores without any subsequent human analysis.

Where no notice has effect, and where a decision which significantly affects an individual is based solely on such automatic processing, the police force must notify the individual that the decision was taken on that basis as soon as reasonably practicable.

In addition, within 21 days of receiving such notification, an individual is entitled by written notice (the 'data subject notice') to require the police force to reconsider the decision or to make a new decision on a different basis.

Within 21 days of receiving the data subject notice, the police force must give the data subject a written response specifying the steps it intends to take to comply with the data subject notice.

The Act provides for the exemption from such provisions of certain decisions reached in this way. These are called 'exempt decisions'. To qualify as an exempt decision certain conditions must be met as follows:

Firstly,

(a) the decision must be taken in the course of steps taken:

for the purpose of considering whether to enter into a contract with the data subject;

with a view to entering into such a contract; or

in the course of performing such a contract; or

(b) the decision must be authorised or required by or under any enactment;

Secondly,

(c) the effect of the decision must be to grant a request of the data subject; or

(d) steps have been taken to safeguard the legitimate interests of the data subject (for example, by

allowing, the data subject to make representations).

Courts may make an order requiring a person taking a decision in respect of the data subject (referred to in the Act as 'the responsible person') to reconsider the decision or to take a new decision which is not based solely on processing by automatic means. Courts will only make such orders if they are satisfied that the responsible person has failed to comply with the data subject notice.

All requests under section 12 will be forwarded as soon as possible upon receipt to the data protection officer to co-ordinate the response.

7.5 Right to Compensation (Section 13)

Any individual who believes they have suffered damage and/or distress as a result of any contravention of the requirements of the Act may be entitled to compensation from a police force where it is unable to prove that it had taken such care as was reasonable in all the circumstances to comply with the relevant requirement.

The Information Commissioner's legal guidance advises:

> 'Damage includes financial loss or physical injury. Unless processing is for the 'special purposes'[52], compensation is not payable for distress alone. If the individual can prove that damage has been suffered, the Court may award compensation for any distress which has also been suffered by reason of the breach of the Act.
>
> Damages for distress alone can be claimed where the contravention relates to the processing of personal data for the 'special purposes'. Again, it is a defence for the data controller to prove that he had taken such care as in all the circumstances was reasonably required to comply with the requirement concerned. There are, however, reduced circumstances in which a contravention may occur as processing only for 'special purposes' is, in certain circumstances, exempt from all but one of the Data Protection Principles and some sections of the Act.'

Examples of breaches that have led to compensation claims:

> *Inappropriate release of the names and photographs of officers working on a sensitive operation by a police force to the media;*
>
> *A serving officer using police-derived information concerning their neighbour's criminal history to rebuke them during the course of an argument witnessed by other neighbours.*

Any claim for compensation arising from this provision will be forwarded to the police force's legal services department (or equivalent) who will liaise, where appropriate, with the data protection officer.

7.6 Right to seek a Court Order for the Rectification, Blocking, Erasure or Destruction of Inaccurate personal data (Section 14)

A data subject has the right to seek a court order for the rectification, blocking, erasure or destruction of inaccurate[53] personal data processed by a police force.

Any court order arising from this provision will be discussed with the police force's legal services department (or equivalent) who will liaise, where appropriate, with the data protection officer and information system owner(s) processing the personal data.

A similar provision under section 12A relates to 'eligible manual data' - manual data which are subject to processing which was already under way immediately before 24th October 1998 - forming part of an accessible record (as defined in section 68). Such eligible manual data is subject to specific rights of

---

[52] The 'special purposes' are defined under DPA section 3 and refer to journalistic or artistic or literary purposes.
[53] See 5.2.3.1 for further guidance on 'accuracy'.

rectification in the period prior to 24th October 2007 where such data are inaccurate or incomplete ("exempt manual data"). The provision under section 12A provides that a data subject may serve a notice in writing on a police force requiring it to rectify, block, erase or destroy exempt manual data which are inaccurate or incomplete, or to cease holding exempt manual data in a way incompatible with the legitimate purposes pursued by the police force. In the event that the police force fails to comply with the notice served by the data subject, the data subject may make an application to a court which may order the police force to take such steps to comply with the notice as the court thinks fit.

7.7 Right to Request an Assessment by the Information Commissioner (Section 42)

Any person can request the Information Commissioner to make an assessment if they believe that they are affected by the processing of personal data by a police force.

Such requests will be made direct to the Information Commissioner who may liaise with the data protection officer in the first instance, with subsequent recourse to the legal services department (or equivalents) as necessary.

Section 42 requests may, in due course, lead to the Information Commissioner serving enforcement notices, information notices and special information notices on police forces. The Information Commissioner also has powers of entry and inspection, all of which is covered in part 5 of the Act.

Where the appeals process related to the use of the exemption under section 28 (national security) the force should contact he ACPO Data Protection Portfolio Secretary.

7.8 Complaints Resolution

One of the routine elements of any data protection officer's role will be the need to co-ordinate the response to complaints and disputes over their police force's processing of personal data.

Though every case will be different it is possible to lay down guidelines which may assist in handling such disputes:

Any person wishing to dispute a police force's processing of personal data should be required to put their case in writing to the data protection officer as the initial point of contact.

Assistance in writing the letter will be offered to the complainant as necessary according to their individual needs (for example, where the complainant cannot write or their first language is not English).

The data protection officer will take reasonable steps to satisfy him/herself with the identity of the complainant as is necessary.

The data protection officer will ensure that a formal process is in place with the professional standards department and other relevant departments in order to establish who will handle the dispute.

Where the issue relates to personal data 'owned' by another police force or organisation the dispute will be directed to that police force or organisation's data protection officer.

Where the dispute relates to information released as part of a Criminal Records Bureau (CRB) disclosure the complainant will be directed to the CRB complaints procedure.

Where the dispute relates to allegations of arrest/conviction information being 'placed on the wrong record' consideration will be given to taking elimination fingerprints to prove/disprove whether the complainant was the person originally arrested/convicted.

If the complaint relates to 'historic' information held on the Police National Computer the person handling the dispute will consider requesting microfiche, where available, from the National Identification Service which may hold additional information.

Consideration will be given to the data subject rights.

Where the dispute relates to personal data processed on a particular information system the matter will be referred to the information system owner.

The information system owner will consult with the data protection officer, specialist colleagues and other information system owners within the force, the Information Commissioner and the ACPO Data Protection & Freedom of Information Portfolios as necessary.

The information system owner will consider relevant police force and national policies and procedures.

The information system owner will strive to deal with the dispute as quickly and thoroughly as possible in the circumstances.

Responses to correspondence will be made in writing and in accord with the police force's agreed timescales for reply.

The data protection officer will attempt to identify any complaint patterns and trends that may indicate that remedial action is required – for example, the provision of further training, guidance or audit.

7.9 Standards

Standard	Source
Police force has adopted measures to respond to subjects' rights as per sections 10, 11 12, 13, 14 of the Act and requests/orders made by the Information Commissioner	7.2-7.7
Police force has developed procedures for the resolving data protection related disputes and complaints	7.8

8 Security and other Protective Measures

8.1 Overview

This chapter examines the obligations placed upon police forces by the seventh data protection principle. In particular it covers:

the relationship between the seventh principle and the ACPO Community Security Policy (CSP);

the relationship between the seventh principle and the ACPO National Vetting Policy for the Police Community;

the need for data processing agreements;

the desirability for data protection compliance to be built into new and amended systems which process personal data;

the requirement for police forces to develop data protection or information system operating rules for their major information systems;

the need for co-ordination between data protection and information security practitioners;

links to chapter 1.

8.2 The Seventh Principle: Introduction

The seventh principle requires that appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

The Act gives some further guidance on matters which must be taken into account in deciding whether security measures are 'appropriate'[54]. These are as follows:

(i) Taking into account the state of technological development at any time and the cost of implementing any measures, the measures must ensure a level of security appropriate to:

(a) the harm that might result from a breach of security; and

(b) the nature of the data to be protected.

(ii) The data controller must take reasonable steps to ensure the reliability of staff having access to the personal data.

There can be no standard set of security measures which collectively achieve compliance with the seventh principle as the appropriate measures will depend on the circumstances. For example, on the harm in a particular case that might result from an unauthorised disclosure of personal data.

Police forces, therefore, need to adopt a risk-based approach to determining what measures are appropriate – effectively a 'balancing act' – and need to consider management and organisational measures as well as technical ones. Further guidance may be found in the ACPO Community Security Policy (CSP).

Police forces will use standard risk assessment and risk management techniques which involve identifying potential threats to the system, the vulnerability of the system to those threats and the necessary

[54] Detailed in schedule 1 part 2 paragraphs 9 and 10.

counter-measures to put in place to reduce and manage the risk.

The police service, through the adoption of the Government Protective Marking Scheme (GPMS) with the Manual of Protective Security (MoPS), provides a mechanism for valuing information assets and affording necessary levels of protection to that information.

The more 'sensitive' the personal data (both as defined under section 2 of the Act – see 3.2.5.1 - and in its wider context), then the greater the protective measures that will need to be put in place. Within policing this is likely to mean that personal data relating to confidential human intelligence resources is likely to be afforded far greater protection than an intranet directory of police headquarters' staff work telephone numbers.

In many cases, a simple consideration of these matters will be sufficient. On the other hand, there are well-established methodologies which will assist police forces in assessing and managing the security risks to theirs systems which can be found in the ACPO CSP. Police forces may consider implementing such controls in the following areas which are expanded upon in the Information Commissioner's legal guidance:

security management;

access controls;

business continuity;

preventing, detecting and dealing with security breaches;

staff selection, vetting and training (see 8.3).

The interpretive provisions of the seventh principle place obligations upon police forces where they use 'data processors' to carry out work which involves the use of personal data, on their behalf (see 8.4).

With regard to the technical and organisational measures to be taken by chief officers in their role as data controllers, the Directive[55] states that such measures must be taken 'both at the time of the design of the processing system and at the time of the processing itself, particularly in order to maintain security and thereby to prevent any unauthorised processing' (see 8.5).

The seventh principle relates to the security of the processing as a whole and the measures to be taken by police forces to provide security against any breaches of the Act rather than just breaches of security.

Responsibility for information security issues will rest with force security boards or equivalent and day-to-day responsibility will lie with the force information security officer. Data protection officers will be consulted on matters relating to personal data.

Exemptions from the seventh principle are summarised in appendix b.

The seventh principle is reflected in Section 3.4 of the Statutory Code of Practice on the Management of Police Information[56], which states:

> "Chief officers should ensure that arrangements within their forces for managing police information include procedures and technical measures to prevent unauthorised or accidental access to, amendment of, or loss of police information. Such procedures should comply with guidance issued under this code unless superseded by regulations made by the Secretary of State under section 53 or section 53A of the Police Act 1996."

[55] The 'Directive' is the European Union Directive 95/46/ED; from which the Act is derived.
[56] The Statutory Code can be found as Appendix 1 in the MoPI Guidance.

8.3 ACPO National Vetting Policy for the Police Community

Police forces are required to comply with the requirements of the ACPO National Vetting Policy for the Police Community in order to help achieve compliance with seventh principle obligations regarding taking 'reasonable steps' to ensure the reliability of employees having access to personal data.

8.4 Data Processing Agreements

The seventh principle places certain obligations on police forces where they use 'data processors[57]' (external organisations or individuals other than their own employees) to carry out work which involves the use of personal data on their behalf.

Likely examples of data processors working for the police:

hardware/software suppliers & maintenance companies;

payroll suppliers;

confidential waste disposal contractors;

other persons working with the police, including volunteers where necessary.

In order to comply with the seventh principle, police forces must;

choose a data processor providing sufficient guarantees[58] in respect of the technical and organisational security measures governing the processing to be carried out, and

take reasonable steps[59] to ensure compliance with those measures, and;

ensure that the processing by the data processor is carried out under a contract, which is made or evidenced in writing (known as a 'data processing agreement'), under which the data processor is to act only on instructions from force, and;

ensure that the data processing agreement requires the data processor to comply with obligations equivalent to those imposed on the chief officer (in his role as 'data controller') by the seventh data protection principle.

ensure that the data processor has notified with the Information Commissioner where necessary.

These obligations will usually be met through the provision of a contract, commonly known as a 'data processing agreement'.

Data processing agreements will specify exactly what the data processor is and is not permitted to do. They will usually cover some/or all of the following areas (which themselves are derived from the data protection principles):

collection;

use & disclosure;

---

[57] 'Data Processor' is defined under DPA section 1.

[58] 'Sufficient guarantees' – The police force is likely to need to evidence that only the relevant personnel will have access to such personal data; that they will have received minimum baseline training in data protection; where appropriate be vetted to ACPO standards; have signed confidentiality agreements; and will have read and understood the obligations imposed under the Data Processing Agreement. The nature of the guarantee will dependant upon the sensitivity of the personal data being processed.

[59] 'Reasonable steps' – These may include undertaking risk assessments, site visits; spot checks and the supervision or management of data processors on police premises.

security;

staff training;

vetting of staff;

confidentiality agreements;

weeding/retention/disposal;

subject access and freedom of Information provisions;

audit/Inspection of data processor by the police;

indemnity.

Data protection officers will be required to provide necessary advice and guidance to assist the police force in choosing data processors that are able to satisfy the technical and organisational standards required by the police service to maintain an appropriate level of protection for the information concerned. Specialist technical advice may be forthcoming form force information security officers. Data protection officers will also advise on the terms and conditions to be included in any contract where the processing of police information is undertaken.

It will be a matter for police forces to decide who will produce necessary agreements. However, it is usually the case that the contracts and purchasing department will have responsibility for the production of any agreements where procurement is involved with any financial implication. In these cases, the data protection officer will be consulted and be expected to provide advice and guidance on the terms and conditions to be included to ensure compliance with the Act's requirements.

It will also be necessary for data protection officers to liaise with contracts and supplies departments to identify occasions where procurement contracts involve access to police information assets or premises in order to ensure appropriate terms and conditions are included in the contract.

There are a number of circumstances where police forces use the services of a data processor but there are no financial considerations included. In such cases, the responsibility to complete a data processing agreement to fulfil the chief officer's responsibilities under the Act may fall to the data protection officer.

Appendices C, D and F contain three documents that will assist police forces' work with regards data processing agreements:

Template and Guidance for a Data Processing Agreement.

Baseline Security requirements for Data Processing Agreements.

Undertaking of Confidentiality.

The ACPO Data Protection Portfolio Group (Disclosure Portfolio Holder) will maintain a central register of all data processing activity known to affect more than one force. This is to assist in the co-ordination of effort, to reduce unnecessary duplication of work by individual data protection officers, and to ensure that a consistent approach can be maintained.

Where police forces identify that a data processor is likely to be carrying out similar processing for other police forces they are requested to inform the ACPO Data Protection Portfolio Group accordingly.

Where the data processor will process personal data outside of the EEA then the eighth principle will

be engaged (see chapter 9)

8.5 Development of, and Changes to, Information Systems

Much of the processing of personal data by police forces is done so using databases and other information technology systems. It is therefore incumbent that those systems are designed to ensure they are compliant with the Act.

Police forces (or those working on their behalf such as PITO, CJIT and the Home Office) will ensure that the development of new, and/or changes to existing, information systems for individual or multiple Police forces occur with due regard to the requirements of the Act, as well as to the Freedom of Information Act (FOIA) and ACPO's Community Security Policy (CSP).

The measures required to achieve compliance are largely identical to those required to ensure that Police information systems fit the business need – police forces require information that is secure, up to date, relevant, adequate, and kept no longer than necessary.

Police forces must also consider data protection and information security requirements at the earliest possible opportunity - usually during the planning stage of a system as part of the identification of the business/user requirement. Compliance must not be seen as an added 'bolt-on' at the latter stages of a project.

8.6 Data Protection/Information System Operating Rules

Information system owners[60], must document how information systems containing personal data under their responsibility will be operated in accordance with the Act.

The documentation, known as 'data protection operating rules' or 'information system operating rules', will set out standards, policies and procedures to ensure that factors such as fair and lawful processing, disclosure, data quality review, retention and disposal, training, security - as required by the principle - are appropriately dealt with.

They can either consist of:

document(s) created for this specific purpose; or,

other pre-existing, or new documents (or references to them) that collectively serve the same purpose.

A template for data protection/information system operating rules can be found at appendix g.

Police forces may wish to include data protection/information system operating rules as an annex to the Risk Management Accreditation Document Sets (RMADS) as required by the ACPO Community Security Policy (CSP).

Police forces will prioritise the review, or creation of data protection/information system operating rules for those information systems containing the most sensitive (both under the Act's definition and generally) and operationally impactive information and personal data

The risk assessment procedure described within the Data Protection Manual of Guidance Part 2: Audit can also be used to assist such a prioritisation process.

Data protection/information system operating rules will be produced by or on behalf of the information system owner. Where required, the information system owner will seek advice on compliance guidance from the data protection officer.

---

[60] Term 'information system owner' is defined under 1.2.5 of this manual.

Data protection officers may quality assure, assess or inspect any documentation produced. Police forces may determine that data protection officers should not formally approve any documentation or data protection operating rules in order to ensure absolute impartiality during any future investigation or audit. However, it is recognised that this may be unavoidable as some data protection officers are also required to perform an accreditor's role. Either way police forces may wish to adopt a formal process for approving data protection operating rules.

Once completed, the data protection/information system operating rules will be made available to all users of the particular information system and the data protection officer, and will be regarded as useful reference material for all users. A central 'library' within the police force may be used to house them. New users of the system must be made aware of all available documentation as part of their system training.

Data protection and other compliance audits will assess compliance with reference to system documentation.

The data protection/information system operating rules will be subject to regular revision and must be amended to reflect significant changes to the system.

Data protection/information system operating rules for nationwide information systems will be developed in accordance with the principles outlined in this chapter by those responsible for the development of RMADSs for those systems.

Data protection/information system operating rules are closely related to Security Operating Procedures (SyOPs). SyOPs provide the rules by which information systems and services must be operated. They notify all authorised users of information systems and services of their compliance responsibilities and unambiguously define only what users can do. They are designed to assist in the efficient and lawful operation of information systems and services and non compliance could lead to administrative, disciplinary or in some cases criminal proceedings being taken.

8.7 Relationship between Data Protection and Information Security Practitioners

In recognition of the anticipated mutual areas of interest and activity, police forces are encouraged to ensure that an effective working relationship exists between the force data protection officer and the force information security officer.

8.8 Responsibilities and Structures

The measures outlined in chapter 1 - including the designation of specific compliance responsibility to certain staff, the provision of data protection training and awareness, the publication of data protection guidance and compliance & quality auditing, and monitoring – are all designed to assist police forces to achieve compliance with their seventh principle obligations.

8.9 Standards

Standard	Source
Police force has effective procedures in place to ensure that force information security boards (or their equivalents) consult with data protection officers when considering the security of personal data	8.2
Police force complies with the ACPO National Vetting Policy for the Police Community	8.3
Police force has effective procedures in place to ensure data processing agreements are developed where required	8.4
Police force has effective measures in place to ensure that data protection and information security requirements are considered during the procurement or development of systems processing personal data	8.5
Police force has produced data protection/information system operating rules for	8.6

systems containing the most sensitive and operationally impactive information and personal data	
Police force ensures that data protection/information system operating rules are made available as necessary to users and other individuals	8.6
Police force has effective procedures in place to ensure that data protection/information system operating rules are subject to regular revision, and are amended to reflect significant changes to the information system	8.6
Police force has ensured that there is effective liaison between data protection and information security officers	8.7

9 Transfers outside the European Economic Area

9.1 Overview

This chapter examines the likely impact of the eighth principle on police forces.

The eighth principle is intended to ensure that data protection considerations cannot be circumvented by transferring personal data to a place where it will enjoy no legal protection and where data subjects will have no rights in respect of it. Transfers can still take place to countries which do not have equivalent data protection legislation where adequacy is ensured by other means in the particular circumstances of the transfer.

9.2 The Eighth Principle

This requires that personal data shall not be transferred to a country or territory outside the European Economic Area (EEA)[61] unless that country or territory ensures an 'adequate' level of protection for the rights and freedoms of data subjects in relation to the processing of their personal data.

The Act does not define 'transfer' but the ordinary meaning of the word is transmission from one place, person, etc to another. Transfer does not mean the same as mere transit. Therefore, the fact that the electronic transfer of personal data may be routed through a third country on its way from the UK to another EEA country does not bring such transfer within the scope of the eighth principle.

On occasions police forces may transfer personal data to UK Government facilities such as embassies or consulates – these are considered to be UK territory and therefore are not transfers beyond the EEA

9.2.1 Schedule 4 and Section 28

Schedule 4 sets out a list of circumstances where the eighth principle does not apply. Collectively these seem to cover the vast majority of instances where the police are likely to transfer personal data beyond the EEA.

In addition, section 28 also provides an exemption from the eighth principle where the application of the exemption is necessary to safeguard national security.

Of the nine conditions within schedule 4, the following are likely to be of most relevance to the police:

(iv) The transfer is necessary for reasons of substantial public interest.

(v) The transfer:-
(a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),
(b) is necessary for the purpose of obtaining legal advice, or
(c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

(vi) The transfer is necessary in order to protect the vital interests of the data subject.

The Information Commissioner has advised that the schedule 4 provisions:

"reflect the fact that there are instances where it will be justifiable to transfer data even though there will be a lower level of protection given to those data. As such, in interpreting these provisions, the derogations should be narrowly construed".

[61] The European Economic Area (EEA) is defined as the European Union countries plus Iceland, Norway, & Liechtenstein. See the European Union website for an up to date listing of its member states and a list of other countries which the European Union has formally accepted as having 'adequate' data protection regimes - http://europa.eu.int/index_en.htm

9.2.2 Adequacy

The interpretive provisions[62] set out a list of factors which must be considered when determining 'adequacy':

a) the nature of the personal data [an acknowledgement that certain types of personal data require greater protection than others];

b) the country or territory of origin of the information contained in the data;

c) the country or territory of final destination of the information;

d) the purposes for which and period during which the data are intended to be processed [this requires a consideration of what will be done with personal data and for how long?];

e) the law, international obligations, codes of conduct or other rules in force in the country or territory in question. With respect to rules and codes of conduct these may be general or made by arrangement in particular cases;

f) any security measures taken in respect of the data in that country or territory.

The Act provides that the European Commission can formally determine which countries and territories outside the EEA have an 'adequate' level of protection[63]. Both the Information Commissioner's website and the European Commission website contain up to date guidance on those countries and territories deemed 'adequate' and further guidance on such transfers.

Any transfer made to a country or territory found to be 'adequate' by the European Commission cannot be a breach of the eighth principle.

If the country beyond the EEA is one with a poor human rights record the protection is more likely to be deemed 'inadequate'.

Where the proposed transfer is to a non-EEA police force then Interpol may be contacted to help make the necessary assessment.

The Public Information Compliance Unit at the Serious Organised Crime Agency (SOCA) may be in a position to provide further advice in the application of the eighth principle to force data protection officers as necessary.

9.2.3 Contractual Conditions

Where the general level of 'adequacy' is found to be insufficient in some limited circumstances contractual conditions similar to those used in data processor agreements (see 8.4) may be applied to a transfer to compensate for those deficiencies. However, such an approach is unlikely to be used by police forces.

Appendix b lists exemptions to the eighth principle.

9.3 Police Force transfers outside the EEA

The eighth principle is unlikely to present a significant barrier to operational policing. Non-operational transfers; for example publication of personal data using force internet services, may need fuller consideration.

---

[62] See DPA schedule 1 part 2 paragraphs 13 to 15.
[63] Such determinations are known as 'Community findings'.

Police forces will adopt a four-stage approach when considering transfers of personal data outside of the EEA (hereafter referred to as transfers to 'third countries') which is described below:

1. Ensure the other seven principles are fully satisfied as required. If they are not, the transfer should not go ahead. Where they are satisfied move on to stage 2 below.

2. Identify whether a schedule 4 condition applies (see 9.2.1). Where one applies the transfer is not precluded by the eighth principle. If a schedule 4 condition cannot be satisfied move on to stage 3 below.

3. Consider whether the third country and the circumstances surrounding the transfer ensure that an 'adequate' level of protection will be given to that data. A decision of whether or not there is adequacy may be based on a European Commission finding of adequacy or after an assessment of adequacy made by the police force itself (see 9.2.2). If adequacy is satisfied the transfer is not precluded by the eighth principle. If not, move on to stage 4 below.

4. Consider whether contractual conditions can be applied to the transfer to compensate for any adequacy deficiencies in order to help safeguard the personal data (see 9.2.3). If such contractual conditions can be made then the transfer is not precluded by the eighth principle. If not, the transfer is precluded by the eighth principle.

The Information Commissioner has produced useful guidance on the eighth principle which can be found on its website. The Department of Constitutional Affairs has also written advice on this subject on its website.

10 Handling Allegations of Criminal Offences under the Act

10.1 Overview

This chapter provides a summary of the criminal offences contained within the Act, with specific detail on those likely to be of most relevance to the Police.

It describes the procedures that the police and the Information Commissioner will follow when criminal offences under the Act are suspected. It explains that those offences fall within three broad groups:

Offence that is not connected to the Police;

Offence or misconduct identified by, or reported to, the Police relating to police-held personal data;

Offence identified by, or reported to, the Information Commissioner relating to police-held personal data.

The chapter is based on the philosophy that there will be a close working relationship between force data protection officers, Professional Standards Departments and the Information Commissioner in order to help safeguard the public's confidence in the Police's use of personal data.

10.2 The Offences

The following offences within the Act have been enabled:

Section 21(1): Failure to notify the Information Commissioner of the processing of personal data;

Section 21(2): Failure to notify the Information Commissioner of relevant changes to the Notification;

Section 24(4): Failure to provide relevant particulars;

Section 47(1): Failure to comply with a Notice;

Section 47(2): Providing false information in response to a Notice;

Section 55(1), (4) and (5): Unlawful obtaining, disclosing or sale of personal data;

Section 59(3): Unlawful disclosure of personal data by the Information Commissioner;

Schedule 9 para 12 & section 60(3): Obstruction of a warrant or failure to assist re warrant execution;

In addition, an offence within the Freedom of Information Act 2000[64] can also apply to personal data:

Section 77 Freedom of Information Act: Altering, defacing, blocking, erasing, concealing any record to prevent disclosure under section 7 (Subject Access).

The following offences have yet to be enabled:

Section 22(6) & 60(2): Assessable Processing without preliminary notification;

Section 56(5): Enforced Subject Access.

[64] Although Scotland has its own legislation, the Freedom of Information (Scotland) Act 2002, section 77 of the Freedom of Information Act 2000 also has effect across Scotland as it applies to the Data Protection Act 1998, itself a UK-wide piece of legislation.

Breaches of the data protection principles are not criminal offences in themselves (although criminal offences are likely to include breaches of the principles). Breaches of the principles will be reported to the data protection officer and information system owner:

In England and Wales, criminal proceedings may only be instigated by the Information Commissioner, or with the consent of the Director of Public Prosecution (Crown Prosecution Service). In Scotland, criminal proceedings will be brought by the Procurator Fiscal. In Northern Ireland, proceedings can be started by the Information Commissioner or by or with the consent of the Director of Public Prosecutions for Northern Ireland.

All offences, with the exception of those relating to the obstruction of a warrant or failure to assist regarding warrant execution, are 'triable either way offences' which can be tried in England or Wales Summarily in the Magistrates' Court or on Indictment in the Crown Court or in Scotland in the Sheriff Court or High Court of Judiciary on Indictment.

A person found guilty of any of these offences can be sentenced on summary conviction to a fine not exceeding the statutory maximum (currently £5,000), or on conviction on indictment, to an unlimited fine.

On conviction of an offender, the Court may order any data apparently connected with the crime to be forfeited, destroyed or erased. Anyone other than the offender who claims to own the material may apply to the Court that such an order should not be made.

The two offences most relevant to the Police are likely to be those under section 55 and, section 77 of the Freedom of Information Act 2000 (see 10.2.1 and 10.2.2).

10.2.1 Section 55

Under section 55(1) a criminal offence is committed if an individual knowingly or recklessly, obtains or discloses personal data, or the information contained in personal data, or procures the disclosure to another person of the information contained in personal data, without the consent of the data controller (chief officer for police forces).

This does not apply where it can be shown that any of the provisions, outlined under section 55(2) shown below, are satisfied:

That the obtaining, disclosing or procuring of the information was either, (i) necessary for the purpose of preventing or detecting crime, or (ii) required or authorised by or under any enactment, by any rule of law, or by the order of a court.

That the individual acted in the reasonable belief that he/she had in law the right to obtain or disclose the data, or to procure the disclosure to the other person.

That the individual acted in the reasonable belief that the data controller (chief officer would have consented if he had known of the obtaining, disclosing or procuring, and the circumstances of it.

That in the particular circumstances, the obtaining, disclosing or procuring was justified as being in the public interest.

Section 78 of the Criminal Justice and Immigration Act 2008 inserts a new defence into section 55 of the Data Protection Act 1998. The defence applies when a person acts for journalistic, literary or artistic purposes with a view to the publication of journalistic, literary or artistic material and in the reasonable belief that their actions were justified as being in the public interest.

Where those working for, or on behalf of, the Police have authority to obtain and disclose personal data in the course of their duties, they will commit section 55 offences if they use their position to obtain, disclose, or procure disclosure of personal data for their own purposes.

In addition to the section 55(1) offence there are further offences under section 55(4) and (5) committed through the selling of personal data - specifically, when a person sells or offers to sell personal data where it has been obtained in contravention of section 55(1). An advertisement indicating that personal data is or may be for sale is an offer to sell. Personal data includes information extracted from personal data for the purposes of these offences.

There are no section 55 offences if the personal data in question falls within the national security exemption (Section 28), or if the personal data is 'category (e) unstructured personal data' as defined by section 68(2) of the Freedom of Information Act 2000[65].

Section 77 of the Criminal Justice and Immigration Act 2008 confers a power on the Secretary of State to make an order altering the maximum penalty for an offence under section 55 of the Data Protection Act 1998. No order has yet been made.

10.2.2 Section 77 FOI Act

Under section 77 of the Freedom of Information Act it is an offence to alter, deface, block, erase, destroy or conceal information and personal data sought under the Subject Access and Freedom of Information Act processes if it is done so with the intention of preventing the disclosure of all or part of the information and personal data sought.

This is a summary offence and is punishable by a fine. A prosecution may be instituted by the Information Commissioner or by the Director of Public Prosecutions (or the Director of Public Prosecutions for Northern Ireland where appropriate).

10.3 Process to be followed

Offences fall within three broad groups and will be handled as described in the following paragraphs.

10.3.1 Offence not connected to the Police

Where a police force receives a complaint that a member of the public or another organisation may have committed or be committing a criminal offence under the Act, the allegation will be recorded by the police force in accordance with the National Crime Recording Standard and associated procedures[66].

Examples of section 55 offences include:

A debt collector impersonating a customer to procure the address of a debtor from a bank;

A call centre operative selling a list of a famous customer's 'friends and family' phone numbers to a journalist.

Where an allegation is made the officer in the case will notify the case to the Head of Investigations at the Information Commissioner:

Address:
The Head of Investigations
Information Commissioner's Office
Wycliffe House
Water Lane

[65] The Freedom of Information (Scotland) Act 2002 (Consequential Modifications) Order 2004 creates an equivalent in Scotland to the new class of personal data created by section 68 of the Freedom of Information Act 2000 in the rest of the UK.
[66] The 'National Crime Recording Standard' (NCRS) should not be confused with the term 'recordable offences'. The NCRS was introduced in 2002 to help ensure consistency between forces as to what crimes are recorded. Section 55 (and section 77 FOIA) offences are not 'recordable offences' (i.e. they are not recorded on the Police National Computer under The National Police Records (Recordable Offences) Regulations 2000 as amended).

Wilmslow
Cheshire
SK9 5AF

Telephone: 01625 545708

Email: investigations@ico.gsi.gov.uk

Where the offence relates solely to data protection matters, the Information Commissioner will deal with the investigation and prosecution.

In the event of offences under the Act being discovered by the Police in the course of their investigations into other matters (e.g. a fraud investigation) it is important that all evidence relating to data protection matters is secured. In such circumstances the Information Commissioner will provide advice as necessary and assist in the preparation of the case file, with regard to any data protection offences.

Where the circumstances of an offence committed under section 55 of the Data Protection Act 1998 may also constitute an offence under the Official Secrets Act 1989, the Police will investigate the matter and submit a file to the Director of Public Prosecution via the Crown Prosecution Service.

The Information Commissioner and/or the OIC will notify the data protection officer of the outcome of the investigation.

10.3.2 Offence or misconduct identified by, or reported to, the Police relating to Police-held personal data

This section concerns the misuse of police-held personal data by those working for or on behalf of a police force.

Examples of section 55 offences include:

A Police Officer carrying out a PNC check on his/her daughter's new boyfriend to help assess his 'suitability';

A member of Police Staff offering to sell police intelligence to a member of a criminal gang;

A cleaner removing computer printouts from the confidential waste and showing them to family members;

A member of Police Staff viewing the custody record of a famous person in custody;

A Police Officer procuring personal data from a bank, using a 'Section 29.3 Form', for his/her own purposes.

In these circumstances, details of the allegation must be forwarded to the police force's Professional Standards Department (PSD).

The PSD will assess the circumstances of the case and identify a proportionate response to the allegation. The assessment will include consideration of all relevant factors including:

The motive of the offender – was it a case of curiosity, was it for personal gain, was it for another person's gain?;

The nature of the personal data – what quantity was involved, what it related to, its sensitivity, and so on;

The harm and/or distress, potential or otherwise, caused to the person to whom the personal data related and others;

The level of intrusion or breach of privacy suffered;

Previous misconduct or criminal breaches by the offender;

Whether the offender was one of many;

The wider public interest.

Where necessary (for example, confirmation that an offence has occurred), the PSD will seek the views of the data protection officer. The Information Commissioner may also be in a position to provide advice. In all cases the data protection officer should be regularly appraised by the PSD of the progress of any investigation and prosecution into offences under the Act.

Having carried out the assessment, the PSD will be in a position to determine the seriousness of the offence. Although it is not possible to draw up definitive criteria to assess that seriousness, the scale of an offence will be apparent.

Those offences deemed to be low-level in nature - for example, a member of staff browsing a record containing a minimal amount of personal data out of curiosity, where there was little prospect of harm or distress – may be dealt with under misconduct only and will not necessarily require a criminal investigation. Each case will need to be assessed against the above criteria.

Those of a more serious nature – for example, a member of staff selling the names and addresses of witnesses in a forthcoming criminal trial to associates of the person charged – are likely to be considered high-level in nature and would be likely to merit a criminal investigation and prosecution.

Where a prosecution is anticipated the PSD will inform the Head of Investigations at the Information Commissioner' Office who will provide guidance and assistance as necessary, though the police force will retain primacy.

A decision by the Crown Prosecution Service not to proceed with a prosecution under the Act should not preclude notification of the case to the Information Commissioner.

The Information Commissioner is particularly keen on pursuing those who procure the disclosure or sale of Police-held personal data.

PSD will notify the data protection officer of the outcome of the case in order that any necessary remedial action can be identified and undertaken by the force.

10.3.3 Offence identified by, or reported to, the Information Commissioner relating to Police-held personal data.

On occasion the Information Commissioner is likely to receive allegations that a police force or individuals working on its behalf have committed offences under the Act.

In such circumstances, the Information Commissioner will take primacy for the investigation and will notify the force's Head of PSD of the complaint. This will allow the police force to consider running a misconduct investigation parallel to or in conjunction with the Information Commissioner's criminal investigation[67].

Where the offender is a senior police officer of ACC or above the Information Commissioner will notify the Chairman of the Police Authority rather than the Head of PSD (or other appropriate authority as per statute).

10.4 The Role of the Information Commissioner's Head of Investigations

[67] In the case of the Police Service of Northern Ireland such allegations should be dealt with by the Ombudsman and Information Commissioner rather than the Force and Information Commissioner.

The Information Commissioner's Head of Investigations' role can be summarised as follows:

To receive from police forces details of offences that are not connected to the Police;

To advise the relevant Head of PSD (or Police Authority in certain circumstances) when the Information Commissioner identifies or receives an allegation of an offence relating to police-held personal data;

To advise the relevant Head of PSD of any Information Commissioner activity or investigation where there is any suspicion there is police officer or police staff involvement. This is to ensure no conflict with Police activity;

To provide the ACPO Data Protection and Freedom of Information Portfolio Holder with statistics and other information relating to all cases referred to the Information Commissioner by police forces.

10.5 Related Offences

The following are related offences that will be considered when dealing with offences under the Act:

Computer Misuse Act 1990, sections 1-3;
Malfeasance in a Public Office (Common Law);
Conspiracy (Section 1(1) Criminal Law Act 1977);
Conspiracy to Pervert the Course of Justice (Section 1(1) Criminal Law Act 1977;
Breach of Confidence (Common Law);
Freedom of Information Act 2000, section 77;
Fraud Act 2006, sections 2 and 4.

10.6 'Victim Care'

Police forces will take appropriate action within their powers and capabilities to mitigate any damage or distress caused to an individual by virtue of any offence under the Act.

10.7 Standards

Standard	Source
Police force has effective procedures in place to ensure that breaches of data protection principles are reported to the data protection officer and information system owner.	10.2
Police force has effective procedures in place to ensure that the Information Commissioner's Head of Investigations is informed of allegations of criminal breaches of the Act as prescribed.	10.3.1
Police force has effective measures in place which ensure that the data protection officer is appraised of the progress of and outcome of all allegations and investigations regarding criminal breaches of the Act.	10.3.2
Police force has procedures in place to ensure that the police force conducts a process to identify any 'lessons learned' at the conclusion of an enquiry in order to identify measures that will be adopted to prevent re-occurrence.	10.3.2
Police force handles allegations of S55 offences by those working for on behalf of a police force in accordance with the procedures described in the MoG.	10.3.2 – 10.6

11 Disclosure of Personal Data by the Police

11.1 Overview

This chapter focuses on the disclosure of personal data by the police to external organisations and individuals. It provides a methodology which data protection officers may follow when considering the data protection aspects of such disclosures (see 11.2 to 11.3).

'Disclosure' may involve the provision of personal data by any means, including; verbally (either at meetings or via the telephone), electronically (email, text, internet, fax) and by the supply of hard copy-documents (letters, memoranda, reports and 'print-outs'). The term 'disclosure' in this chapter should not be confused with the rules for disclosure as provided by the Criminal Proceedings Investigations Act 1996 (CPIA) or the Civil Procedures Rules.

The chapter examines requests by the police for the disclosure of personal data from other bodies and organisations using a standard form and the exemption under section 29.3 of the Act (see 11.5). A brief examination of disclosures required by law can be found at 10.6, while 10.7 introduces forthcoming work to produce an A-Z reference of disclosure/information sharing for the police service. Standards relating to disclosure can be found at 10.8.

Related guidance on 'information sharing' may be found in section 6 of the MoPI Guidance.

11.2 Introduction

Disclosures of personal data can be divided into various types based upon the legal basis underlying them as shown in the diagram below. The whole diagram represents all disclosures by the police. The second 'row' on the diagram shows that those disclosures can be divided into those under statute (yellow side) and those under common law (green side). The third 'row' shows that the statutory disclosures can be further divided into those where there is an obligation or compulsion to disclose and those where there is a power to disclose, but not an obligation. Finally, the bottom row provides some examples of disclosures in the three categories.

All Disclosures		
	Statutory	**Common law**
Obligation Requires disclosure	**Power** Gives the option/discretion (i.e. the power) to disclose, but does not compel	where there is a pressing social need and it is necessary and proportionate to do so for policing purposes – public interest test
e.g.	e.g.	e.g.
Child Support Agency Subject Access Court Order	Statutory partners [Section 115 Crime and Disorder Act 1998] CRB [Part V Police Act 1997]	Crimewatch, any individual or body, And, currently for: notifiable occupations

11.3 Approach to disclosures of personal data

This section provides a summary of the various relevant factors which should be considered in order to help ensure disclosure decisions are data protection compliant.

The diagram below summaries the process, while the subsequent paragraphs up to 10.4 provide further explanation.

Define the personal data (see 11.3.1)

Define the purpose (see 11.3.1)

Define the recipient (see 11.3.1)

Identify the legal basis/power to disclose (see 11.3.1)

Apply the data protection principles (see 11.3.2)

Apply other considerations (see 11.3.3)

11.3.1 Define the personal data, the recipient, the purpose and the legal basis/power

The personal data under consideration for disclosure should be identified.

The identity of the recipient of the personal data should be confirmed.

The specific purpose or purposes for the disclosure should be identified.

The legal basis/power to disclose should be established.

11.3.2 Application of the data protection principles

Each of the principles needs to be considered. Where it appears unlikely that the disclosure can satisfy the requirements of a principle it is necessary to consider any relevant exemptions that provide relief from all or parts of the principles. If a principle still cannot be satisfied then the disclosure must be reconsidered. In some cases modifications to the contents of the disclosure (i.e. providing less or different personal data) may help achieve the necessary compliance.

The factors identified in the following table may be a useful prompt when considering the principles:

Fair and lawful processing

What is the purpose(s) of the disclosure?
What processing operations are involved?
Who is the data controller?
Who else processes the personal data? Their status?
What personal data is to be disclosed?
What sensitive personal data is to be disclosed?
What are the lawful grounds for disclosure?
Are there any prohibitions from disclosure?
Can a schedule 2 (& 3 if needed) condition be met?
How will the disclosure be fair?
How will the 'fair processing requirements' be met?
Which exemptions can be employed?
Is the disclosure compatible with the original purpose(s)?

Data Quality

Is the information to be disclosed 'fit for purpose?

Have reasonable steps been taken to ensure that the information to be disclosure is adequate, relevant and not excessive for the intended purpose?
How will the personal data be used if disclosed?
Does the proposed disclosure contain any information that
is not necessary for the identified purpose?
Have reasonable steps been taken to ensure that the information proposed for disclosure is accurate and up to date?
What level of confidence applied to the disclosure?
What consideration has been given to the grading of the information (5x5x5)?
Due consideration should be given to the date the information was recorded or the date of the event, and the time elapsed since.

Review, Retention and Disposal

How long will the recipient of the disclosure retain that personal data?
Is it appropriate to stipulate conditions for its review, retention and disposal?

Subject Rights

How will the disclosure be recorded for audit purposes?
Do any Section 10 notices apply?

Security

To whom is the proposed disclosure being made?
Is there a 'need to know' (e.g., is it necessary for them to fulfil official duties)?
Have conditions been specified for the use of the information to be disclosed (including any secondary use)?
Is the disclosure to be made by approved secure means (e.g., not over insecure email links)?

Overseas Transfers

How will the proposed disclosure be sent outside the European Economic Area?
If so, how will the eighth principle be satisfied?

11.3.3 Other considerations

Having considered the principles it is also useful to consider other factors before finally determining the appropriateness of a disclosure. The following may assist:

Proportionality

Would the benefit of disclosure outweigh the possible harm that may be caused by the disclosure?

Further care will be taken to ensure that only the minimum personal data is disclosed and where necessary disclosed documents are redacted to remove irrelevant content.

Third Parties

Have details of third parties been removed from the disclosure where necessary?

No information, which gives personal details of any third-party, should be disclosed unless it is felt necessary and a balancing exercise weighing the rights of the data subject against the wider public interest (or some case the rights of the other party) has been fully documented. Alternatively, the information may be disclosure where third-party consent is sought and agreed.

Views of Officer in the Case (OIC)

Have the views of the OIC been considered?

In some instances the disclosure may link to a specific police enquiry and it is often useful to consult with the OIC for his/her opinion on disclosure. An OIC may also hold additional background information that can assist the decision-making.

Non-Prejudicial

Can it be confirmed that the proposed disclosure would not prejudice ongoing criminal proceedings or investigations?

Reasonable checks should be made to ensure that the disclosure would be not be likely to prejudice any ongoing criminal proceedings or current police investigations (or possible investigations by other agencies such as HM Revenue and Customs).

Where it is identified that there are current criminal proceedings, the Crown Prosecution Service should be consulted.

Clarity

Care must be taken to ensure that the disclosure will not be misinterpreted, and that it is clear which elements of the disclosure are factual and which are not. The disclosure should be credible, clear and capable of being substantiated if challenged; be from a credible source; and be presented in a balanced and neutral fashion, but in such a way that its significance was readily apparent.

Approval of the decision

Has the disclosure been approved by an officer at an appropriate level/position within the police force?

A decision as to whether or not to provide personal data that may significantly affect an individual or individuals must be authorised at the appropriate level.

The levels of authority for disclosure should be identified in local force policy and will be determined by the nature and circumstances of the disclosure in each particular case. The approval to disclose should be escalated to chief officer level where there is no predetermined delegated authority.

The nature of the disclosure, local policies and procedures, information sharing agreements will readily identify the appropriate level for the formal decision-making on the disclosure.

Method of Disclosure

Has an appropriate method of disclosure been identified?

Recognising that disclosures may be made verbally (either face to face meetings or via the telephone), electronically (email, text, internet, fax) or by the provision of hard copy-documents (letters), all staff need to ensure that appropriate records are maintained for any disclosure made.

Depending on the nature and circumstances of the disclosure, a chief officer may need to consider informing the person to whom the information relates that a disclosure is intended to be made. In such cases, it may be appropriate to allow a period of time before the disclosure is made for the person concerned to appeal, to seek an injunction against the disclosure or make other representations as necessary.

However, police forces should be cognisant that whatever conditions may be applied to a disclosure,

once the disclosure has been made the control of the personal data is effectively lost.

Audit Trail

In case of future challenge is there is an auditable decision-making trail to support any decision to disclose?

It is desirable to have an audit trail to identify what disclosures have been made at any time. Such records can include the information requested and the information disclosed, the requestor and recipient of the disclosure, the person authorising the disclosure and the rationale leading to the decision to disclose (or not as may be the case).

Cause and Effect

There should be an obvious 'cause and effect' link between the proposed disclosure and the purpose. Personal data should only be disclosed if there is clear reason to believe that it may be materially relevant – i.e. not fancifully, remotely or speculatively relevant. Personal data should not be disclosed on the basis that, although there is no apparent reason to believe that it is relevant, it could conceivably turn out to be.

The use of de-personalised information

In some instances it will become apparent that the purpose(s) of the disclosure can be achieved without the need to disclose personal data. In those cases, it is good practice to provide de-personalised information, though of course relevant factors such as those in this table must not be overlooked. In addition, this approach must not used where it is believed that the recipient of the de-personalised information may have the ability to 're-create' the personal data using other information they are likely to have access to.

11.4 Nationally approved Memoranda of Understanding and Policy

Over recent years ACPO has endorsed a number of memoranda of understanding with external bodies, including government departments and agencies, and industry associations. Many of these documents include procedures for the routine disclosure of police information, including personal data, between the signatories and, where these exist, the identified procedures will be followed.

It has been agreed that ACPO will maintain a registration system for recording all ACPO guidance and practice advice to ensure that they are properly available and reviewed as required. All such documents and advice will be published on the ACPO Intranet. The ACPO Data Protection Portfolio Group [Disclosure Portfolio Holder] will also make these available and provide advice as required.

11.5 Personal Data Request Form (section 29)

The police service has used a form referred to in many police forces as a 'Section 29(3) Form' or a 'Data Protection Form' to request personal data and other information from other agencies. This manual introduces a replacement to that form, which is now known as a 'Personal Data Request Form' and can be found at appendix f.

11.6 Disclosures required by law or made in connection with legal proceedings etc. (section 35)

11.6.1 Section 35: Introduction

The very nature of policing means that police forces hold personal data whose disclosure to other bodies or individuals is either required by law, or is sought by those considering or undertaking legal proceedings. In this context section 35 recognises that the public interest may require the disclosure of personal data, which would otherwise be in breach of the Act, where the disclosure is required by law or made in connection with legal proceedings etc.

Section 35 has three key provisions:

Firstly, the provisions within section 35(1) cover mandatory disclosures of personal data required by law;

Secondly, those within section 35(2) deal with discretionary disclosures of personal data in connection with legal proceedings;

Thirdly those at section 35A (introduced by the Freedom of Information Act 2000) concern parliamentary privilege are unlikely to be of relevance to police forces and are not covered by this document.

The provisions within section 35(1) and 35(2) provide relief from the 'non-disclosure provisions' which are explained in more detail in 10.6.2.

11.6.2 The non-disclosure provisions

The non-disclosure provisions are defined at section 27(3) and section 27(4) of the Act. They are a various elements from the Act which tend to impose a restriction on the disclosure of personal data and are detailed in the subsequent paragraphs. The provisions within section 35(1) and 35(2) provide relief from them, though it is important to note that the relief is only to the extent to which they are inconsistent with the disclosure in question - in other words police forces can only disregard any or all of the non-disclosure provisions if their application would prejudice the disclosure, and then they can only be disregarded to the extent necessary.

The non-disclosure provisions are as follows:

the first principle, except where it requires compliance with the conditions in schedules 2 and 3 (legitimate processing conditions and sensitive personal data conditions); and,

the second, third, fourth and fifth principles; and,

section 10 (right to prevent processing likely to cause damage or distress); and sections 14 (1) to (3) (rectification, blocking, erasure and destruction);

to the extent to which they are inconsistent with the disclosure in question.

11.6.3 Section 35(1): Disclosures required by law

11.6.3.1 Section 35(1): Overview

Section 35(1) exempts personal data from the non-disclosure provisions (see 11.6.2) to the extent to which they are inconsistent with the disclosure in question, where the disclosure is required by or under any enactment, by any rule of law or by the order of a court.

In this context an 'enactment' refers to an Act of Parliament or a statutory instrument; while an 'order of a court' refers to an order of any court or tribunal that has the status of a court. It is difficult to identify any disclosure from the police service required 'by any rule of law' which would not also be one required either under 'enactment' or 'order of a court'.

Clearly, the relief provided by section 35(1) is conditional in nature:

firstly, individually each of the non-disclosure provisions can only be disregarded to the extent necessary; and,

secondly, the remaining parts of the Act must be considered, perhaps including a need to comply with some of the non-disclosure provisions, and a need in all cases for a schedule 2 (and on

occasions a schedule 3) condition, and for compliance with the sixth, seventh and eight principles (where applicable).

With regards to the first principle the Information Commissioner has recently stressed the importance of fairness to data subjects even where a disclosure is required by law. Their legal guidance states:

> 'In these circumstances, the legal obligation overrides any objection which the data subject may have, but an element of fairness can still be applied. For example, if the data controller is well aware when he collects the data that at some point he is likely to have to make disclosures of those data under statute, it would not be incompatible with the disclosure to notify data subjects at the time the data are collected from them, that such disclosure is likely. The First Principle should not, be disapplied generally.'

Police forces need to have processes in place for recognising and processing disclosures of personal data where section 35(1) is engaged, and for establishing new procedures as further relevant legislation is enacted. Those processes should be designed to ensure that any disclosure of personal data is done so in compliance with the remaining parts of the Act from which section 35(1) does not provide relief. They should also ensure that where requests/demands are received that are perceived as being too broad-brush, vague or unclear they are challenged and the necessary clarity provided so that the Police force is confident that the required disclosure is appropriate. Police forces are also encouraged to ensure that fair processing notices (see 3.2.3.2 and 3.2.3.3) explain, where necessary, the likely disclosures that would be made under law.

Some court orders may be considered 'unsatisfactory' by a police force for reasons such as ambiguity over what personal data was actually required, or because the disclosure would impinge on operational activity or cause harm in some other manner. Police forces should therefore have in place systems that will ensure that where an 'unsatisfactory' court order requiring disclosure of personal data is received the police force is in a position to exercise its ability to seek to vary the court order where necessary.

11.6.3.2 Section 35(1): Examples

Within the policing context this provision will be engaged in the following examples:

Enactment: A mandatory disclosure of personal data relating to an individual's criminality by a police force to the Criminal Records Bureau, as required by Part V the Police Act 1997;

Enactment: A mandatory disclosure of personal data relating to a police officer's salary by their police force to the Child Support Agency, as required by The Child Support (Information, Evidence and Disclosure) Regulations 1992;

Enactment: A mandatory disclosure of individual sickness data relating to staff by a police force to the Home Office NMIS Data Hub, a requirement derived from Section 44(1) of the Police Act 1996;

Order of a Court: A mandatory disclosure of conviction antecedents by a police force to a Family Proceedings Court, as required by an order issued by a District Judge.

11.6.3.3 Section 35(1): Schedules 2 and 3

Under section 35(1) the necessary schedule 2 conditions most likely to be relied upon by police forces are one or more of the following:

3. The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.

5. The processing is necessary-
(a) for the administration of justice,
(b) for the exercise of any functions conferred on any person by or under any enactment,
(c) for the exercise of any functions of the Crown, a Minister of the Crown or a government

department, or
(d) for the exercise of any other functions of a public nature exercised in the public interest by any person.

Under section 35(1) where a schedule 3 condition is required, the most likely to be relied upon by police forces are one or more of the following:

1. The data subject has given his explicit consent to the processing of the personal data.

6 The processing-
(a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),
(b) is necessary for the purpose of obtaining legal advice, or
(c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

7(1) The processing is necessary-
(a) for the administration of justice,
(aa) for the exercise of any functions of either House of Parliament,
(b) for the exercise of any functions conferred on any person (including a constable) by or under an enactment, or
(c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department.

(SI 2000 No 417) 10. The processing is necessary for the exercise of any functions conferred on a constable by any rule of law.

11.6.3.4 Section 35(1): Considering a disclosure request

As a general rule, when a request for the disclosure of personal data is received by a police force, and it is identified that section 35(1) is engaged, it may be useful if the relevant factors described under 10.3.2 and 10.3.3 plus the following are considered as part of a disclosure decision-making process:

Has the requirement under law for the disclosure been confirmed?
What personal data is involved?
What are the schedule 2 (and where necessary schedule 3) grounds for processing?
How will the disclosure comply with sixth principle rights where exercised?
How will the disclosure comply with seventh principle?
Is the proposed method for disclosure appropriate in terms of information security?
In the case of a court order, should the police force seek to vary the court order?
To what extent do each of the non-disclosure provisions need to be disregarded?
Where a non-disclosure provision does not need to be completely disregarded how will compliance with it be achieved?

11.6.4 Section 35(2): Disclosures made in connection with legal proceedings

11.6.4.1 Section 35(2): Overview

Section 35(2) exempts personal data from the non-disclosure provisions (see 11.6.2) to the extent to which they are inconsistent with the disclosure in question, where the disclosure is necessary:

for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings);

or for the purpose of obtaining legal advice;

or is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

Whereas section 35(1) compels disclosure, a police force is not obliged to disclose personal data pursuant to a request made by a third party under section 35(2), but may chose to do so dependant on the circumstances.

Clearly, the relief provided by section 35(2) is conditional in nature:

> firstly, individually each of the non-disclosure provisions can only be disregarded to the extent necessary that would still permit the disclosure; and,
>
> secondly, the remaining parts of the Act must be considered, perhaps including a need to comply with some of the non-disclosure provisions and a need in all cases for a schedule 2 (and on occasions a schedule 3) condition, and for compliance with the sixth, seventh and eight principles (where applicable).

Section 35(2) requires that the disclosure should be 'necessary', as opposed to being simply desirable. The Act does not define 'necessary'. Sufficient evidence would need to be provided to confirm the necessity of a disclosure.

The Act does not define 'legal proceedings' and perhaps more importantly does not define what would constitute 'prospective legal proceedings'. Clearly, 'legal proceedings' would include criminal and civil cases, but may include employment tribunals, discipline cases, evictions and extradition hearings.

Police forces may reasonably require that evidence is provided to substantiate 'prospective legal proceedings', such as a letter from a solicitor.

The Information Commissioner's legal guidance states:

> 'This provision affords the data controller exemption from any or all of the non-disclosure provisions in cases where: the data controller is satisfied that the nature of the request is such that the disclosure of the personal data falls within this section i.e. the disclosure is necessary for one or more of the above, and the data controller is satisfied that to apply the particular provision would be inconsistent with the disclosure in question.
>
> The data controller has to remember that Schedule 2 and (where the processing is of sensitive personal data) Schedule 3 still have to be complied with. In many cases, the data controller will not be in a position to make a decision as to whether the necessity test can be met, or will not wish to make the disclosure because of his relationship with the data subject, with the result that the requesting party will have to rely upon a Court order to obtain the information'.

The discretionary nature of the exemption means that police forces are encouraged to develop policies that identify in what circumstances they are likely to exercise that discretion and those where they are unlikely to do so

11.6.4.2 Section 35(2): Examples

Within the policing context this provision will be engaged in the following examples:

> *A discretionary disclosure of the name and address of a convicted offender by a police force to the victim of the offender, in order that the victim can institute civil proceedings;*
>
> *A discretionary disclosure of the name and address of a shoplifter who received an adult caution by a police force to the shop, in order that the latter can institute civil retail recovery proceedings;*
>
> *A discretionary disclosure of the name and address of the owner of a dog who details were obtained when the police attended a non-crime incident involving their dog attacking another dog resulting in substantial vet bills, in order that proceedings could be instituted to recover those costs.*

11.6.4.3 The police's approach to section 35(2)

The discretionary element to this exemption means that there is a risk of inconsistent, and potentially unfair, use of the exemption within a police force and between police forces. Although the nature of the exemption means that every case needs to be judged on its merits it is advisable for police forces to adopt a general position identifying the likely circumstances in which they may choose to exercise their discretion in this area and disclose.

Forces are therefore encouraged to develop documentation that describes their approaches to requests for, or disclosures of, personal data where section 35(2) is likely to be engaged. Such documentation is likely to be developed cognisant of issues such as:

A recognition that disclosures are at the discretion of the Chief Officer;

A recognition of individuals' and organisations' right to request information for use in civil proceedings, balanced against a recognition that forces' own resource limitations mean that a prioritisation process needs to take place;

What type of request will receive priority – for example those necessary to protect vulnerable persons, and those made by victims of crime seeking redress against offenders;

What types of request are likely to be declined – for example those that are spurious, 'fishing expeditions', disproportionately onerous or where the force is not convinced that they meet the section 35(2) criteria;

A recognition that disclosures will not normally be made until the conclusion of any related criminal investigation or prosecution, and the circumstances where the CPS or Coroner will be consulted;

A recognition that disclosures will not be made that may prejudice a completed, ongoing, planned or potential investigation or prosecution;

Consideration that that the force may not wish to undertake to provide a précis or summary of larger documents, or rather may provide copies of documents appropriately redacted;

Recognition that disclosures will be based upon careful consideration of all the facts, including the public interest, the risk of harm to individuals or investigations, the requirements of legislation and the force's business requirements for disclosures;

Recognition of the fair processing requirements to 'third party' individuals whose personal data may form part of the requested information;

The circumstances in which statements provided by police officers will and will not be disclosed;

The circumstances in which statements provided by third parties will and will not be disclosed;

The circumstances in which the request will be processed under the Subject Access provisions;

Proof of identity requirements;

An appropriate decision-making model, such as that described under 10.3 above and 10.6.4.5 below;

The circumstances in which fees may be charged.

11.6.4.4 Section 35(2): Schedules 2 and 3

Under section 35(2) the necessary schedule 2 conditions most likely to be relied upon by police forces

are one or more of the following:

1. The data subject has given his consent to the processing.

5 The processing is necessary for-
(a) for the administration of justice.

6(1) The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

Under section 35(2) where a schedule 3 condition is required, the most likely to be relied upon by police forces are on or more of the following:

6 The processing-
(a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),
(b) is necessary for the purpose of obtaining legal advice, or
(c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

7(1) The processing is necessary-
(a) for the administration of justice,

11.6.4.5 Section 35(2): Considering a disclosure request

As a general rule, when a request for the disclosure of personal data is received by a police force, and it is identified that section 35(2) is engaged, it may be useful if the relevant factors described under 10.3.2 and 10.3.3 plus the following are considered as part of a disclosure decision-making process:

Has the requirement under law for the disclosure been confirmed?
What personal data is involved?
What are the schedule 2 (and where necessary schedule 3) grounds for processing?
How will the disclosure comply with sixth principle rights where exercised?
How will the disclosure comply with seventh principle?
Is the proposed method for disclosure appropriate in terms of information security?
In the case of a court order, should the police force seek to vary the court order?
To what extent do each of the non-disclosure provisions need to be disregarded?
Where a non-disclosure provision does not need to be completely disregarded how will compliance with it be achieved?

Guidance on section 35 has been promised by the Information Commissioner.

11.7 'A to Z' Disclosure Reference

A working group is developing an 'A to Z' reference of disclosure/information sharing. It is intended to provide a useful resource identifying standard routes for disclosure of personal data and other information across the police service. The working group will report progress to the ACPO Data Protection Portfolio Holder. The need for the 'A to Z' has been identified by police data protection officers.

11.8 Standards

Standard	Source
Police force has processes in place for recognising and processing disclosures of personal data where section 35(1) is engaged.	11.6.3

Police force has processes in place for recognising and processing disclosures of personal data where section 35(2) is engaged.	11.6.4

12 Powers of the Information Commissioner

12.1 Overview

The data protection powers of the Information Commissioner's Office are to:

Conduct assessments to check organisations are complying with the Act;

Serve information notices requiring organisations to provide the Information Commissioner's Office with specified information within a certain time period;

Serve enforcement notices and 'stop now' orders where there has been a breach of the Act, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;

Prosecute those who commit criminal offences under the Act;

Conduct audits to assess whether organisations processing of personal data follows good practice; and

Report to Parliament on data protection issues of concern.

Appeals from notices are heard by the Information Tribunal, an independent body set up specifically to hear cases concerning enforcement notices or decision notices issued by the Information Commissioner.

Full details of the Information Commissioner's powers can be found on their website: www.ico.gov.uk

12.2 The Criminal Justice and Immigration Act 2008

Section 144 of the Criminal Justice and Immigration Act 2008 inserts new sections 55A to 55E into the Data Protection Act 1998. These new sections create a framework for the Information Commissioner to serve a monetary penalty notice on a data controller.

New section 55A(1) gives the Information Commissioner a discretion to serve a monetary penalty notice on a data controller if the Commissioner is satisfied there has been both a serious contravention by the data controller of the data protection principles and that the contravention was of a kind likely to cause substantial damage or substantial distress. The Commissioner must also be satisfied that the contravention was deliberate or that the data controller knew or ought to have known that there was a risk that the contravention would occur (and that it would be of a kind likely to cause substantial harm or substantial distress) but failed to take reasonable steps to prevent it occurring (new section 5A(2) and (3)).

New section 55A(5) and (9) make provision for the Secretary of State to make regulations prescribing the maximum amount of the penalty.

New section 55B makes provision for the procedural rights of data controllers served with a monetary penalty notice. This includes a duty on the Information Commissioner to serve a data controller with a notice of intent that he proposes to issue a monetary penalty notice. This will allow a data controller to make representations before any monetary penalty notice is imposed. It also provides a right of appeal to the Information Tribunal against a monetary penalty notice issued or the amount specified in a monetary penalty notice. By new section 55B(3) and (6), the Secretary of State may make regulations prescribing what must be contained in notices of intent.

New section 55C requires the Information Commissioner to prepare and issue guidance on how he proposes to exercise his functions in respect of notices of intent and monetary penalty notices. The

guidance, and all alterations and replacements, must be approved by the Secretary of State, and laid before Parliament.

New section 55D makes provision for the enforcement of monetary penalty notices.

New section 55E confers a power on the Secretary of State to make an order to make further provision in connection with monetary penalty notices and notices of intent. No order has yet been made.

Appendix A: Standards

Standard	Source
ACPO/Senior Manager lead on data protection matters identified within the police force.	1.2.2
Data protection officer appointed or nominated within the police force and responsibilities documented.	1.2.4
Information system owners formally identified for key systems within the police force and tasked.	1.2.5
Effective reporting lines established within the police force.	1.3
Data protection training provided for all staff within the police force.	1.4
Data protection guidance published within the police force.	1.5
Data protection auditing and monitoring carried out in accordance with the ACPO Data Protection Manual of Guidance Part 2: Audit.	1.6
Police force has considered the need for 'fair processing notices' in the scenarios described.	3.2.3.4
Police force has notified to the Information Commissioner using the standard Notification.	3.3.2
Police force has established a process to resolve fair and lawful processing disputes and complaints.	3.4
Police force has adopted measures to ensure that any personal data processed is adequate, relevant, not excessive, accurate, and kept up-to-date.	5.2
Police force has adopted procedures to ensure that personal data is reviewed and disposed/ retained/de-personalised when no longer required.	5.3.1
Police force has established a process to resolve data quality disputes/complaints.	5.4
The ACPO standard subject access application form is freely available to enquirers/applicants.	6.4
Police force handles 'National' applications in accord with the ACPO-NIS SLA.	6.5
Police force has adequate procedures in place to inform subject access applicants with 'unsatisfactory' applications of that fact in a timely manner.	6.6
Police force has adequate procedures in place to handle 'local' subject access applications.	6.6-6.9
Police force has adequate procedures for ensuring that CPIA requirements are satisfied where required.	6.11
Police force has sound procedures to update or augment existing records, or create new records, with information obtained from subject access applications.	6.12
Police force has established a subject access appeals/complaints process.	6.13
Police force has robust procedures in place to ensure subject access application information is retained only as long as necessary.	6.14
Police force has adopted measures to respond to subjects' rights as per sections 10, 11 12, 13, 14 of the Act and requests/orders made by the Information Commissioner.	7.2-7.7
Police force has developed procedures for the resolving data protection related disputes and complaints.	7.8
Police force has effective procedures in place to ensure that force information security boards (or their equivalents) consult with data protection officers when	8.2

considering the security of personal data.	
Police force complies with the ACPO National Vetting Policy for the Police Community.	8.3
Police force has effective procedures in place to ensure data processing agreements are developed where required.	8.4
Police force has effective measures in place to ensure that data protection and information security requirements are considered during the procurement or development of systems processing personal data.	8.5
Police force has produced data protection/information system operating rules for systems containing the most sensitive and operationally impactive information and personal data	8.6
Police force ensures that data protection/information system operating rules are made available as necessary to users and other individuals	8.6
Police force has effective procedures in place to ensure that data protection/information system operating rules are subject to regular revision, and are amended to reflect significant changes to the information system	8.6
Police force has ensured that there is effective liaison between data protection and information security officers.	8.7
Police force has effective procedures in place to ensure that breaches of data protection principles are reported to the data protection officer and information system owner.	10.2
Police force has effective procedures in place to ensure that the Information Commissioner's Head of Investigations is informed of allegations of criminal breaches of the Act as prescribed.	10.3.1
Police force has effective measures in place which ensure that the data protection officer is appraised of the progress of and outcome of all allegations and investigations regarding criminal breaches of the Act.	10.3.2
Police force has procedures in place to ensure that the police force conducts a process to identify any 'lessons learned' at the conclusion of an enquiry in order to identify measures that will be adopted to prevent re-occurrence.	10.3.2
Police force handles allegations of S55 offences by those working for on behalf of a police force in accordance with the procedures described in the MoG.	10.3.2 – 10.6
Police force has processes in place for recognising and processing disclosures of personal data where section 35(1) is engaged.	11.6.3
Police force has processes in place for recognising and processing disclosures of personal data where section 35(2) is engaged.	11.6.4

Appendix B: Exemptions

The purpose of this appendix is to provide a quick route for identifying the exemptions that may be available to data protection practitioners. Each exemption will be carefully read and considered on a case-by-case basis before it is employed. Section 38 of the Act provides a power for the Lord Chancellor to make orders providing exemptions where disclosure of information is statutorily prohibited or restricted, subject to certain conditions.

Provision for which an exemption is sought	Exemption can be found under
1st Principle - Fair and Lawful Processing [Entire]	Section 28 National Security Section 32 Journalism Literature & Art Section 33A Manual Data held by Public Authorities Section 36 Domestic Purposes
1st Principle - Fair and Lawful Processing (To the extent to which it requires compliance with Para 2 of Part II of Schedule 1) [fair obtaining/processing notice] Part of the Subject Information Provisions defined under Section 27.2	Section 28 National Security Section 29.2 Crime & Taxation (Statutory Functions) Section 30 Health Education & Social Work Section 31 Regulatory Functions Section 32 Journalism Literature & Art Section 33A Manual Data held by Public Authorities Section 34 Information available to the public by or under enactment Section 36 Domestic Purposes Section 38.2 Powers to make further exemptions by order- yet to be exercised Schedule 7.2 Armed forces [where prejudicial to combat effectiveness] Schedule 7.3 Judicial Appointments & Honours Schedule 7.4 Crown Employment and Crown or Ministerial Appointment Schedule 7.5 Management Forecasts Schedule 7.6 Corporate Finance Schedule 7.7 Negotiations [with the Data Subject] Schedule 7.10 Legal Professional Privilege
1st Principle - Fair and Lawful Processing (Except to the extent to which it requires compliance with Schedules 2 & 3) Part of the Non-Disclosure Provisions defined under Section 27.3 and 4	Section 28 National Security Section 29.1 Crime & Taxation Section 29.3 Crime & Taxation Section 32 Journalism Literature & Art Section 33A Manual Data held by Public Authorities Section 34 Information available to the public by or under enactment Section 35 Disclosures required by law or made in connection with legal proceedings Section 36 Domestic Purposes Section 38.2 Powers to make further exemptions by order- yet to be exercised
2nd Principle - Obtained for specified and lawful purposes & not processed incompatibly Part of the Non-Disclosure Provisions defined under Section 27.3 and 4	Section 28 National Security Section 29.3 Crime & Taxation Section 32 Journalism Literature & Art Section 33 Research, History & Statistics Section 33A Manual Data held by Public Authorities Section 34 Information available to the public by or under enactment Section 35 Disclosures required by law or made in connection with legal proceedings Section 36 Domestic Purposes Section 38.2 Powers to make further exemptions by order- yet to be exercised

3rd Principle - Relevant & Not Excessive Part of the Non-Disclosure Provisions defined under Section 27.3 and 4	Section 28 National Security Section 29.3 Crime & Taxation Section 32 Journalism Literature & Art Section 33A Manual Data held by Public Authorities Section 34 Information available to the public by or under enactment Section 35 Disclosures required by law or made in connection with legal proceedings Section 36 Domestic Purposes Section 38.2 Powers to make further exemptions by order- yet to be exercised
4th Principle - Accurate and Up to Date Part of the Non-Disclosure Provisions defined under Section 27.3 and 4	Section 28 National Security Section 29.3 Crime & Taxation Section 32 Journalism Literature & Art Section 33A Manual Data held by Public Authorities (partial) Section 34 Information available to the public by or under enactment Section 35 Disclosures required by law or made in connection with legal proceedings Section 36 Domestic Purposes Section 38.2 Powers to make further exemptions by order- yet to be exercised
5th Principle – Retained no longer than Is necessary Part of the Non-Disclosure Provisions defined under Section 27.3 and 4	Section 28 National Security Section 29(3) Crime & taxation Section 32 Journalism Literature & Art Section 33 Research, History & Statistics Section 33A Manual Data held by Public Authorities Section 34 Information available to the public by or under enactment Section 35 Disclosures required by law or made in connection with legal Section 36 Domestic Purposes Section 38.2 Powers to make further exemptions by order- yet to be exercised
6th Principle – Processed in accordance with Data Subjects' rights	Section 28 National Security Section 32 Journalism Literature & Art Section 33A Manual Data held by Public Authorities (partial) Section 36 Domestic Purposes
7th Principle - Protected	Section 28 National Security Section 33A Manual Data held by Public Authorities Section 36 Domestic Purposes
8th Principle – Not transferred to territories lacking appropriate protection to Data Subjects' rights and Freedoms	Section 28 National Security Section 32 Journalism Literature & Art Section 33 Research, History & Statistics Section 33A Manual Data held by Public Authorities Section 36 Domestic Purposes Schedule 4 Cases where the Eighth Principle does not apply
Section 7 - Right of Access to personal data Part of the Subject Information Provisions defined under Section 27.2	Section 9A: Appropriate Fees Limit (Unstructured personal data) Section 29.1 Crime & Taxation Section 29.2 Crime & Taxation [Statutory Functions] Section 29.4 & 5 Crime & Taxation [Council Tax, Housing Benefit etc.] Section 30 Health Education & Social Work Section 31 Regulatory Functions Section 32 Journalism Literature & Art Section 33A Manual Data held by Public Authorities (partial) Section 33 Research, History & Statistics Section 34 Information available to the public by or under enactment Section 36 Domestic Purposes

	Section 38.1 Powers to make further exemptions by order- yet to be exercised Schedule 7.1 Confidential References given by the Data Controller Schedule 7.2 Armed forces [where prejudicial to combat effectiveness] Schedule 7.3 Judicial Appointments & Honours Schedule 7.4 Crown Employment and Crown or Ministerial Appointment Schedule 7.5 Management Forecasts Schedule 7.6 Corporate Finance Schedule 7.7 Negotiations [with the Data Subject] Schedule 7.8 Examination Marks Schedule 7.9 Examination Scripts Schedule 7.10 Legal Professional Privilege Schedule 7.11 Self Incrimination
Section 10 - Right to prevent processing likely to cause Damage or Distress Part of the Non-Disclosure Provisions defined under Section 27.3 and 4	Section 28 National Security Section 29.3 Crime & Taxation Section 32 Journalism Literature & Art Section 33A Manual Data held by Public Authorities Section 34 Information available to the public by or under enactment Section 35 Disclosures required by law or made in connection with legal proceedings Section 36 Domestic Purposes Section 38.2 Powers to make further exemptions by order- yet to be exercised
Section 11 - Right to prevent processing for purposes of Direct Marketing	Section 28 National Security Section 33A Manual Data held by Public Authorities Section 36 Domestic Purposes
Section 12 - Rights in relation to Automated Decision-Making	Section 28 National Security Section 32 Journalism Literature & Art Section 33A Manual Data held by Public Authorities Section 36 Domestic Purposes
Section 13 - Compensation for failure to comply with certain requirements	Section 28 National Security Section 33A Manual Data held by Public Authorities (partial) Section 36 Domestic Purposes
Section 14 (1) to (3) - Rectification, Blocking, Erasure and Destruction Part of the Non-Disclosure Provisions defined under Section 27.3 and 4	Section 28 National Security Section 29.3 Crime & Taxation Section 32 Journalism Literature & Art Section 33A Manual Data held by Public Authorities (partial) Section 34 Information available to the public by or under enactment Section 35 Disclosures required by law or made in connection with legal proceedings Section 36 Domestic Purposes Section 38.2 Powers to make further exemptions by order- yet to be exercised
Part III - Notification	Section 28 National Security Section 33A Manual Data held by Public Authorities Section 36 Domestic Purposes
Part V - Enforcement	Section 28 National Security
Section 55 - Unlawful obtaining etc of personal data	Section 28 National Security Section 33A Manual Data held by Public Authorities

Appendix C: Template and Guidance for a Data Processing Agreement

Introduction

The following template and guidance are provided to assist Data Protection Officers where they may be required to draw up an agreement to fulfil the Chief Officer's obligations under Schedule 1 Part II, Sections 11 and 12. Data Protection Act 1998.

Each heading contains advice notes followed by standard wording which may be useful.

This information is provided as a guide only, as the circumstances on each occasion will vary and the content is required to reflect those unique circumstances.

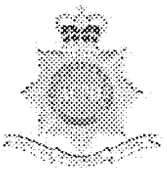
Advice and guidance on how to prepare the Agreement is written in red italics to make it easy for users to edit the document.

Standard wording is provided which may or may not be relevant on each occasion. Data Protection Officers are encouraged to exercise caution when preparing the draft agreement to consider each clause on its individual relevance to the processing in question. Depending on the nature and circumstances of the business requirement, Agreements may need to be more or less comprehensive than others.

Where financial issues arise, it is likely that you may only be required to provide advice and guidance on the terms and conditions for the processing of police information, to be included in a procurement contract and you will therefore need to liaise with appropriate contract staff within your Force.

This template is provided for force Data Protection Officers only and is not recommended for wider use.

Data Protection Officers are encouraged to consult with the business managers responsible for the processing of the relevant information, in the first instance, to prepare an initial draft based on the template and the subsequent completion/approval of that Agreement will be a matter for local arrangements.



DATA PROCESSING AGREEMENT

THIS AGREEMENT is made the [*add date*] day of *[add month year]*

BETWEEN

The Parties

- *Add details of the relevant parties*
- *The following wording may assist:-*

The Chief Constable of *[relevant force],* (herein after called the "Data Controller") of [*address]* of the one part and

[add details of third party data processor] (herein after called the "Data Processor"), *[add address]* on the behalf of *[add details if appropriate]* (herein after called *[add details as appropriate])* of the other part.

Purpose

- *It is necessary to define the purpose of the processing. This must be consistent with an official notified purpose. It is useful also to specify how this linked to current policing objectives.*
- *The following wording may assist:-*

The purpose of the disclosure is to facilitate ..... by *[add]* commissioned by *[add],* to undertake *[add purpose]* as attached in the *[add title of document and add any relevant documentation to support the business initiative as an appendix)]* at Appendix X ("the Purpose").

This Agreement sets out the terms and conditions under which Data held by the Data Controller will be disclosed to the Data Processor. This Agreement is entered into with the purpose of ensuring compliance with the Data Protection Act 1998 ("the Act"). Any processing of data must comply with the provisions of this Act.

The Purpose is consistent with the original purpose of the Data collection.

The Processing of Data for the Purpose will assist the Data Controller to fulfil his obligations under *[add basis e.g., Section 17 Crime and Disorder Act 1998 to exercise their functions with due regard to the likely effect of the exercise of those functions on, and the need to do all that it reasonably can to prevent crime and disorder in its area*].

Definitions

- *It is necessary to define any terms or phrases used throughout the document to ensure clarity of agreement.*
- *Ensure all references to the definitions are consistent throughout the document*
- *The following wording may assist:*

The following words and phrases used in this Agreement shall have the following meanings except where the context otherwise requires:

The expressions "**Data**", "**Data Controller**", "**Data Processor**", "**Personal Data**", "**Sensitive Personal Data**", "**Processing**", "**Information Commissioner**", have the same meaning as in Sections 1, 2, and 6 of The Data Protection Act 1998, as amended.

"**Police Data**" *[or "Test Data" or "Research Data"]* means any Data including "Personal Data" and

"Sensitive Personal Data" as above provided by the Data Controller to the Data Processor and as identified in the schedule at Appendix *(add where necessary)*.

"**Aggregated Data**" means Police Data *[or "Test Data" or "Research Data"]* grouped together to the extent that no living individual can be identified from that Aggregated Data or any other Data in the possession of, or likely to come into the possession of any person obtaining the Aggregated Data.

"ACPO" means the Association of Chief Police Officers.

The recipient(s) of the research findings (including Aggregated Data) for the purposes of this Agreement is/are: *[add]*.

The "**Designated Police Manager**" means [*Name of designated police manager with day to day responsibility for the management of the Purpose]* on behalf of the Data Controller or other such person as shall be notified to the Data Processor from time to time.

The **"Project Manager"** means *[add name of person with day to day management responsibility]* on behalf of the Data Processor or such other person as shall be notified to the Data Controller from time to time.

"Government Protective Marking Scheme" means a scheme for the classification of information.

"Agreement" means this data processor agreement together with its Schedules and all other documents attached to or referred to as forming part of this agreement.

"Charges" means the amounts due and payable by the Data Controller to the Data Processor for the provision of the Services as calculated in accordance with Schedule <>.

"Confidential Information" means any information relating to the Data Controller's customers and prospective customers, current or projected financial or trading situations, business plans, business strategies, developments and all other information relating to the Data Controller's business affairs including any trade secrets, know-how and any information of a confidential nature imparted by the Data Controller to the Data Processor during the term of this Agreement or coming into existence as a result of the Data Processor's obligations, whether existing in hard copy form or otherwise, and whether disclosed orally or in writing. This definition shall include all Personal Data.

"Services" means the services to be provided by the Data Processor during the term of this Agreement, as described in Schedule <>.

Headings are inserted for convenience only and shall not affect the construction or interpretation of this Agreement and, unless otherwise stated, references to clauses and schedules are references to the clauses of and schedules to this Agreement;

Any reference to any enactment or statutory provision shall be deemed to include a reference to such enactment or statute as extended, re-enacted, consolidated, implemented or amended and to any subordinate legislation made under it; and

The word 'including' shall mean including without limitation or prejudice to the generality of any description, definition, term or phrase preceding that word, and the word 'include' and its derivatives shall be construed accordingly.

Information provision

- *Define the nature and parameters of the information subject to processing under the terms of this Agreement.*
- *You may wish to consider referencing an appendix with a comprehensive list of the information if this clarity is required in any given circumstances.*

- *Define the time periods for the processing if appropriate.*
- *Use this Section to clarify ownership of the information and any circumstances in which the Data Controller is prepared to relinquish that ownership.*
- *The following wording may assist:*

It is recognised that the Purpose requires access to the Data, which has been previously protectively marked by the Data Controller under the Government Protective Marking Scheme.

The Police Data will be provided over a set time period to be agreed in advance by both Parties as identified in the schedule attached at Appendix *(add where necessary).*

Ownership of the Police Data shall at all times remain with the Data Controller.

Use, Disclosure and Publication

- *Define any restrictions to be placed on the data processor regarding the use and disclosure of the police information*
- *Consider if there are any issues regarding contact with individual's which may be identified from the police information*
- *Consider if there are any data matching issues*
- *Consider if there are any other processing issues which may be likely to cause damage or distress to any data subject*
- *Consider if there are any other documents or standards which may be relevant to the processing*
- *Consider if there are any issues concerning the publication of information connected with the Purpose and what conditions the Data Controller may wish to impose on the data processor in this respect.*
- *The following wording may assist:*

The Police Data will be used solely for the Purpose and *[add specific circumstances].*

Subject to clause x below, the Police Data will NOT be matched with any other Personal Data otherwise obtained from the Data Controller, or any other source, unless specifically authorised in writing by the Data Controller.

The Police Data will NOT be disclosed to any third party without the written authority of the Data Controller except as in accordance with clause x below.

Access to the Police Data will be restricted to those employees of the Data Processor as listed in Appendix (add where necessary) and approved by the Data Controller, directly involved in the processing of the Police Data in pursuance of the Purpose.

No steps will be taken by the Data Processor to contact any Data Subject identified in the Police Data.

Personal Data used for research will not be published in identifiable form unless the persons concerned have given their consent and in conformity with other safeguards laid down by domestic law.

Data Protection and Human Rights

- *Consider the necessity to identify designated persons responsible for these issues for both Parties*
- *Consider if Subject Access considerations apply*
- *Consider if Freedom of Information considerations apply*
- *The following standard wording may assist:*

The use and disclosure of any Personal Data shall be in accordance with the obligations imposed upon the Parties to this Agreement by the Act and the Human Rights Act 1998. All relevant codes of practice or data protection operating rules adopted by the Parties will also reflect the data protection practices of each of the parties to this Agreement.

The Parties agree and declare that the information accessed pursuant to this Agreement will be used and processed with regard to the rights and freedoms enshrined within the European Convention on Human Rights. Further, the Parties agree and declare that the provision of information is proportional, having regard to the purposes of the Agreement and the steps taken in respect of maintaining a high degree of security and confidentiality.

The Parties undertake to comply with the provisions of the Act and to notify as required any particulars as may be required to the Information Commissioner.

The receipt by the Data Processor from any Data Subject of a request to access to the Data covered by this Agreement must be reported immediately to the person nominated below representing the Data Controller, who will arrange the relevant response to that request.

If any Party receives a request under the subject access provisions of the Act and personal data is identified as belonging to another Party, the receiving Party will contact the other Party to determine if the latter wishes to claim an exemption under the provisions of the Act.

It is acknowledged that where a data controller cannot comply with a request without disclosing information relating to another individual who can be identified from that information, he is not obliged to comply with the request, unless;

a) the other individual has consented to the disclosure of the information to the person making the request; or
b) it is reasonable in all the circumstances to comply with the request without the consent of the other individual. In determining whether it is reasonable, regard shall be had, in particular, to:-

- any duty of confidentiality owed to the other individual;
- any steps taken by the data controller with a view to seeking consent of the other individual;
- whether the other individual is capable of giving consent;
- any express refusal of consent by the other individual.

If any Party receives a request for information under the provisions of the Freedom of Information Act 2000 identified as belonging to another Party, the receiving Party will contact the other Party to determine whether the latter wishes to claim an exemption under the provisions of that Act.

Where the Data Processor receives a request for information under the provisions of the Freedom of Information Act 2000 in respect of information provided by or relating to the Data Controller, the Data Processor will contact the person nominated below to ascertain whether the Data Controller wishes to claim any exemption including the determination of whether or not the Data Controller wishes to issue a response neither to confirm nor deny that information is held.

Where any Party receives a Notice under Section 10 of the Act, that Party will contact the person nominated below to ascertain whether or not to comply with that Notice.

The following personnel are authorised by the Parties to assume responsibility for data protection compliance, notification, security, confidentiality, audit and co-ordination of subject rights and Freedom of Information:

The Data Processor shall give reasonable assistance as is necessary to the Data Controller in order to enable him to:

- Comply with request for subject access from the Data Subjects;
- Respond to Information Notices served upon him by the Information Commissioner;
- Respond to complaints from Data Subjects;
- Investigate any breach or alleged breach of the Act.

in accordance with his statutory obligations under the Act.

Nominated Post holder *Relevant force*

On reasonable notice, periodic checks may be conducted by the Data Controller to confirm compliance with this Agreement.

Confidentiality

- *Consider what confidentiality issues apply*
- *Consider what special terms and limitations may be necessary to impose on the data processors to prevent any likely damage or distress caused to data subjects*
- *The following standard wording may assist:*

Except as specified in clause X below, the Data Processor shall not use or divulge or communicate to any person (other than those whose province it is to know the same for the Purpose, or without the prior written authority of the Data Controller) any Data obtained from the Data Controller, which it shall treat as private and confidential and safeguard accordingly.

The Data Processor shall ensure that any individuals involved in the Purpose and to whom Police Data is disclosed under this Agreement are aware of their responsibilities in connection with the use of that Police Data and have confirmed so in writing.

For the avoidance of doubt, the obligations or the confidentiality imposed on the Parties by this Agreement shall continue in full force and effect after the expiry or termination of this Agreement.

Respect for the privacy of individuals will be afforded at all stages of the Purpose.

Clause X above shall not apply where disclosure of the Police Data is ordered by a Court of competent jurisdiction, or subject to any exemption under the Act, where disclosure is required by a law enforcement agency or regulatory body or authority, or is required for the purposes of legal proceedings, in which case the Data Processor shall immediately notify the Data Controller in writing of any such requirement for disclosure of the Police Data in order to allow the Data Controller to make representations to the person or body making the requirement.

The restrictions contained in clauses X and X shall cease to apply to any Data which may come into the public domain otherwise than through unauthorised disclosure by the Parties to the Agreement.

Retention, Review and Deletion.

- *Consider how long the data is required to be retained by the data processor*
- *Set appropriate parameters for retention and disposal of police information consistent with any security conditions imposed below.*
- *Identify the title or post holder responsible for the retention, review and deletion of police data subject to this agreement.*
- *Consider what conditions will apply to the data processor and relevant police managers*

Security

- *Consider what guarantees are required from the data processor in respect of the technical and organisational security measures governing the processing to be carried out.*
- *Consider what arrangements are necessary to reduce any identified risks*
- *Consider what specific terms and conditions need to apply to the processing in question*
- *Consider where the processing is to take place, on what premises etc.,*

- *Identify who will be responsible for the security both on behalf of the data processor and the data controller*
- *Consider how the police information will be transferred to the data processor and in what format. I.e., CD, disc, print out, by courier, secure email, etc.,*
- *Consider any necessary terms for passcode management*
- *Consider what arrangements are necessary for secure disposal of police information*
- *Consider what technical back up arrangements (including archived data) may occur and how these will be securely managed*
- *Consider what vetting requirements may apply in accordance with ACPO Vetting Policy*
- *Consider if the data processors will visit police premises or require access to any other police assets*
- *Consider referencing system operating procedures where security arrangements are complex*
- *Consider what arrangements may be necessary where the data processor may engage the services of sub-contractors, including cleaning and maintenance staff.*
- *Consider what audit and inspection arrangements may be necessary to ensure that the terms of this Agreement are fulfilled*
- *Consider how security breaches will be managed (you may wish to stipulate that the security incident reporting form is used – see annex A).*

The Data Processor recognises that the Data Controller has obligations relating to the security of Data in his control under the Act, ISO7799 and the ACPO Information Community Security Policy. The Data Processor will continue to apply those relevant obligations as detailed below on behalf of the Data Controller during the term of this Agreement.

The Data Processor agrees to apply appropriate security measures, commensurate with the requirements of principle 7 of the Act to the Data, which states that: "appropriate technical and organisation measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data". In particular, the Data Processor shall ensure that measures are in place to do everything reasonable to:

- make accidental compromise or damage unlikely during storage, handling, use, processing transmission or transport
- deter deliberate compromise or opportunist attack, And
- promote discretion in order to avoid unauthorised access

During the term of this Agreement, The Project Manager shall carry out any checks as are reasonably necessary to ensure that the above arrangements are not compromised.

The Data Controller may wish to undertake suitability checks on any persons having access to police premises and the Police Data and further reserves the right to issue instructions that particular individuals shall not be able to participate in the Purpose without reasons being given for this decision. The Data Processor will ensure that each person who will participate in the Purpose understands this and provides their written consent as necessary.

The Data Processor will ensure that the personal data accessed is not used other than as identified within this agreement, and that the agreement is complied with.

The Data Controller reserves the right to undertake a review of security provided by any Data Processor and may request reasonable access during normal working hours to the Data Processor premises for this purpose. Failure to provide sufficient guarantees in respect of adequate security measures will result in the termination of this Agreement.

Access to the Police Data will be confined to authorised persons only. These will be the individual identified in the documentation attached at Appendix *(add where necessary).*

The Data Processor undertakes not to use the services of any sub-contractors in connection with the processing of the Police Data without the prior written approval of the Data Controller.

Indemnity

- *Consider what indemnity may be appropriate and consult legal advisors where necessary.*
- *The following wording based on Home Office Guidance may assist:*

In consideration of the provision of the Police Data for the Purpose the Data Processor undertakes to indemnify and keep indemnified the Data Controller against any liability, which may be incurred by the Data Controller as a result of the Data Processor's breach of this Agreement.

Provided that this indemnity shall not apply:

(a) where the liability arises from information supplied by the Data Controller which is shown to have been incomplete or incorrect, unless the Data Controller establishes that the error did not result from any wilful wrongdoing or negligence on his part
(b) unless the Data Controller notifies the Data Processor as soon as possible of any action, claim or demand to which this indemnity applies, commits the Data Processor to deal with the action, claim or demand by settlement or otherwise and renders the Data Processor all reasonable assistance in so dealing;
(c) to the extent that the Data Controller makes any admission which may be prejudicial to the defence of the action, claim or demand.

Disputes

- *The following wording based on Home Office Guidance may assist:*

In the event of any dispute or difference arising between the Parties out of this Agreement, the Designated Police Manager and the Project Manager or the persons appointed pursuant to clause 9.3 of this Agreement shall meet in an effort to resolve the dispute or difference in good faith.

The Parties will, with the help of the Centre for Dispute Resolution, seek to resolve disputes between them by alternative dispute resolution. If the Parties fail to agree within 56 days of the initiation of the alternative dispute resolution procedure, then the Parties shall be at liberty to commence litigation.

Term, Termination and Variation

- *Specify an end date for the Agreement. This should be within a realistic period to allow for the arrangements to be properly managed and reviewed where appropriate.*
- *The following wording based on Home Office Guidance may assist:*

The Data Controller may at any time by notice in writing terminate this Agreement forthwith if the Data Processor is in material breach of any obligation under this Agreement.

At the discretion of the Data Controller this Agreement shall terminate after the replacement of the Project Manager.

Either Party may terminate this Agreement by giving 30 days notice in writing to the other Party.

The Data Controller will have the final decision on any proposed variation to this Agreement. No variation of the Agreement shall be effective unless it is contained in a written instrument signed by both Parties and annexed to this Agreement.

Miscellaneous

- *The following wording based on Home Office Guidance may assist:*

This Agreement acts in fulfilment of part of the responsibilities of the Data Controller as required by paragraphs 11 and 12 of Schedule 1, Part II of the Data Protection Act 1998.

This Agreement constitutes the entire agreement between the Parties as regards the subject matter hereof and supercedes all prior oral or written agreements regarding such subject matter.

If any provision of this Agreement is held by a Court of competent jurisdiction to be invalid or unenforceable, such invalidity or unenforceability shall not affect the remaining provisions of this Agreement, which shall remain in full force and effect.

The validity, construction and interpretation of the Agreement and any determination of the performance which it requires shall be governed by the Laws of England and the Parties hereby submit to the exclusive jurisdiction of the English Courts.

Signed on behalf of the Chief Constable of [relevant force}

.....

In the presence of.....

Signed on behalf of .....

In the presence of .....

Annex A to Appendix C

Security Report

From

To Force Data Protection Officer
Relevant force

Date

Location of Premises:

Person Reporting:

Date and time of occurrence/came to notice:
Brief details including impact :

Appendix D: Baseline Security requirements for Data Processing Agreements

Introduction

All Chief Constables are committed to compliance with the ACPO/ACPOS Community Security Policy, which was based on the British Standard for Information Security Management (BS7799), now superseded by BS27001.

The basic requirements for a data processing agreement are specified below. Additional safeguards may be specified according to the sensitivity and classification of the data and the circumstances of the Data Processing Agreement.

Section 1 Information Security Policy

A written statement of Information security policy should be available for the organisations involved in the Agreement.

Please attach a copy of your organisation's Information Security Policy.

Section 2 Information Security Organisation

Responsibility for information security should be allocated to an individual within the organisation. That individual should be operating within a management framework that initiates and controls the implementation of information security.

Please advise who has designated responsibility for information security within your organisation and describe their role and the management framework within which they operate.

Section 3 Assets Classification and Control

It is important to maintain appropriate protection of the computer and information assets used by the data processor.

Please list below the hardware, software and information, which will be used for the purposes of the Agreement.

What accountability for these assets is in place? Who will be the nominated System Owner of these assets for the purpose of the Agreement?

Section 4 Personnel Security

The Chief Constable will need to ensure the reliability of any persons having access to data.

How has the reliability of persons subject to this agreement been assessed?

Any persons having access to data as part of this agreement may be required to give consent to background enquiries in accordance with Force policy. Please provide written consent as required.

Please confirm that all persons connected with this project have received training and awareness in Data Protection and information security. A confidentiality clause will be included in the Agreement which all persons involved may be required to sign.

Please confirm that all persons involved with this project are made aware of the procedure for reporting any security breaches, threats, weaknesses of malfunctions that might impact on the security of the data.

Section 5 Physical and Environmental Security

Appropriate measures should be in place to prevent unauthorised access or unlawful processing, accidental loss, destruction or damage.

Please advise details of the premises used for this purpose and in relation to each named premises:-

a) What access controls are there to the buildings?	
b) What access controls are there to the rooms?	
c) Are the windows lockable when accessible from the outside?	

d) Is the door lockable where the information is stored?	
e) Is information secured in a lockable cabinet when not in use?	
f) Is there a clear desk policy in relation to this information?	
g) Do outside contractors/maintenance/cleaning staff have access to the room?	
h) Is the information visible to unauthorised individuals, i.e., through windows, from corridors etc.,?	
i) Is there any intention to use portable computers for this purpose? If so, what special control measures will be deployed to protect data?	
j) Is the computer/server used to store data in connection with the project physically secured in any way(e.g., by cable to desk etc.)?	

[Please copy for additional premises as necessary]

Section 6 Computer and Network Management

In addition to the physical security outlined above, please provide details of the following:-

a) Is the computer a stand-alone? If not, What measures are taken to prevent unauthorised access via your network or from external networks?	
b) Is there a policy and procedure for the disposal of sensitive material (computer or otherwise)? What procedure is in place to ensure that the data is cleansed from computer media as it becomes obsolete for whatever reason? What procedure is in place to ensure that data held on computer media is handled appropriately when equipment is sent for repair?	
c) Are system security procedures regularly audited?	

d) Are there documented rules for the use of this system available for all users? If so, do users sign to show they have read and understood the Rules?	
e) What control measures are in place to prevent the introduction of malicious software to the system (e.g., computer viruses)?	

Section 7 System Access Controls

a) Are there controls on the system to prevent unauthorised access (i.e. Is there a mechanism for the identification and authorisation of individual users, e.g., user ID and password)?	
b) Is there an automatic log-out after an appropriate time interval?	
c) Is there a warning at log-on to forbid unauthorised use of the system?	
d) Is there an audit trail to identify who has accessed the system including time, date and which records were accessed?	
e) Who monitors the audit trails? How long are they retained and how is the security of the audit trails maintained?	

Section 8 Systems Development and Maintenance

All information systems used as part of this agreement should be designed from the outset with information security in mind to cover, as a minimum, the control measures contained in this document.

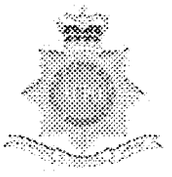
Section 9 Business Continuity Planning

a) Is there an effective backup and recovery mechanism to secure the data? And, where is this held?	
b) What security surrounds these back-up facilities?	

Section 10 Compliance

Agreements must comply with appropriate legal requirements and the prevailing policies of all parties involved.

Appendix E: Undertaking of Confidentiality



Undertaking of Confidentiality

I [name of individual] as an employee of the data processor involved in the research as defined in the Agreement between the [Relevant force] and [add details] to which this Undertaking is appended, hereby acknowledge the responsibilities arising from this Agreement.

I understand that my part in fulfilling the Purpose means that I may have access to the Data and that such access shall include

reading or viewing of information held on computer or displayed by some other electronic means,

reading or viewing manually held information in written, printed or photographic form, or

overhearing any radio, telephone or verbal communication.

I undertake that;-

I shall not communicate to nor discuss with any other person the contents of the Data except to those persons authorised by the Data Controller as is necessary to progress the agreed Purpose.

I shall not retain, extract, copy or in any way use any Data to which I have been afforded access during the course of my duties for any other purpose.

I will only operate computer applications or manual systems that I have been trained to use. This training will include the requirements of the Data Protection Act 1998 which prescribes the way in which personal data may be obtained, stored and processed.

I will comply with the appropriate physical and system security procedures made known to me by the Data Processor.

I will act only under instruction from the [add details of postholder] or other relevant official in the processing of any Data.

I understand that the Data is subject to the provisions of the Data Protection Act 1998 and that by knowingly or recklessly acting outside the scope of this Agreement I may incur criminal and/or civil liabilities.

I undertake to seek advice and guidance from the [add details of postholder] or other relevant official of the Data Controller in the event that I have any doubts or concerns about my responsibilities or the authorised use of the Data defined in the Agreement

I have read, understood and accept the above.

Name.....

Signature.....

Date.....

Appendix F: Personal Data Request Form

Introduction

For many years the police service has used a form referred to in many police forces as a 'Section 29(3) Form' or a 'Data Protection Form' to request personal data and other information from other agencies. This appendix introduces a replacement to that form, which is now known as a 'Personal Data Request Form'.

Section 29(3) of the Data Protection Act 1998 does not create any power for a person to request information. Section 29(3) permits the disclosure of personal data which would otherwise be precluded by particular elements of the Act (known as the 'non-disclosure provisions') in cases where the failure to disclose would prejudice the prevention or detection of crime or the apprehension or prosecution of an offender. Effectively it allows organisations and individuals to disclose personal data to the police, where it is necessary to do so to prevent or detect crime, apprehend or prosecute offenders, without fear of themselves breaching the Act.

The police's power to request information comes in the main from the Police Act and other pieces of legislation which enable police officers or police staff to carry out their duties, e.g. Police and Criminal Evidence Act 1984 (PACE), Criminal Procedures Investigations Act 1996 (CPIA), etc. together with common law powers. The Police Act 1996, section 30(1) gives constables all the powers and privileges of a constable throughout England and Wales. Section 30(5) defines powers as powers under any enactment whenever passed or made. These powers include the investigation and detection of crime, apprehension and prosecution of offenders, protection of life and property and maintenance of law and order. Under the Police Reform Act 2002, the chief officer can delegate certain powers to police staff.

This new Personal Data Request Form has been devised for completion by police officers or police staff when personal data is required in connection with their policing duties. It has been developed in consultation with the Information Commissioner and is endorsed by the ACPO Data Protection Portfolio Group. Completion of the form will ensure a consistent approach by the police forces in their legitimate data gathering objectives. However, other organisations which are approached for personal data by the police may still insist on their own versions of the form being completed and this should be acceded to as necessary.

The previous form has been in use for many years and consideration will need to be given to not only raising awareness among police officers and staff of the existence of the new form but also to informing your many partner organisations so that they can make their staff who are likely to receive requests for the disclosure of personal data from the police using these forms aware that the format has changed.

Completing the Personal Data Request Form

The person completing the form should: -

- Fill in the form clearly and comprehensively as the other organisation or individual needs sufficient information to decide whether to disclose the personal data and any other information or not;

- Give as much information as possible to assist the other organisation or individual to locate the personal data and other information that is required without compromising the investigation. If information is only of interest from a certain time period that should be specified;

- Use a more general statement such as "On-going police investigation into a serious incident" and get the form signed by a Superintendent or above where the investigation is of such a nature that it is not appropriate to disclose further detail;

- In the table tick all of the purpose boxes which are relevant, and if none apply complete the

"other" section. (See below for examples covered by these boxes);

- Send the form to a designated point of contact, where one exists, in the organisation holding the personal data and other information. If one has not been identified the organisation should be contacted to establish who would be most appropriate. A targeted request is more likely to be dealt with efficiently and comprehensively;

- Determine which is the most appropriate way to submit the form, e.g. in person, by phone, by fax, by letter, by email or some other medium. This decision should consider factors such as the sensitivity of the enquiry and the personal data sought, and take into account the Government Protective Marking Scheme (GPMS) classification and the appropriate handling guidelines. The form should also indicate how any of the disclosed personal data should be provided to the police, taking into account how it might impact upon the GPMS classification.

The counter signatory should ensure that the form: -

- Is filled in clearly;

- Gives sufficient information but will not compromise any investigation;

- Ensure that the request falls within the purpose(s) and legal basis(s) as identified in the table;

- That appropriate security has been applied.

In their absence the person completing the form should ensure those requirements have been met.

Action if the personal data is not disclosed

The form now contains a response section. If the personal data is not disclosed the person completing the form may: -

- Be able to provide additional details required by the organisation/individual to locate the personal data requested;

- Wish to identify a person within the organisation who is responsible for data protection issues and refer the request to them for further consideration;

- Wish to consider whether the individual is deliberately obstructing a police officer acting in the execution of their duty (section 89 of the Police Act 1996). This obstruction must be a positive act which prevents or makes it more difficult for an officer to carry out his/her duty. It may not be an individual's specific purpose to obstruct, provided that he/she is aware that his/her intended act would do so.

- Apply to the court for a disclosure order, in which case a copy of the completed form with the response can be supplied with the other papers as part of this request.

Examples of types of enquiries and the most appropriate purposes

For the prevention, investigation and detection of crime
This will cover a large percentage of requests and is fairly self-explanatory. However, one example might be the scenario where an unconscious female is removed to hospital and the police need to determine if she has been the victim of a spiked drink. Information will be required from a doctor at the hospital to ascertain if a crime has been committed.

For the apprehension and prosecution of offenders
Again this is a very common type of request. An example is where the police have details of a suspect and require information from the employer to enable them to make an arrest.

To confirm or corroborate information for intelligence purposes
Intelligence has been received which suggests that a certain property is being used for human trafficking. The investigation is at an early stage and information may be sought from a number of sources to progress the enquiries. One such request may be directed to the Housing Benefits Section for the details they may hold of individuals claiming benefits whilst residing at the property.

To put before a court to obtain a search warrant
An investigation into drug dealing has identified a suspect and addresses which may be in use for dealing. Information is required to firm up this intelligence prior to applying to the court for a search warrant.

To prepare a file for the Coroner's Court
Following a fatality or sudden death, the police are required to prepare a file for the Coroner and may require information from doctors, employers, etc in order to carry out this duty.

To further a money laundering or confiscation investigation
This is self explanatory.

To risk assess an address to safeguard the health and safety of any emergency personnel attending
A 999 call is received from neighbours reporting sounds of breaking glass, shouting, etc. and suspect that a serious domestic incident is taking place. Police and ambulance are en route. The most recent available information shows one of the occupants to have been admitted for psychiatric assessment and treatment. Information is sought from the health service to ascertain whether this person is still in their care or may have returned to the address; if they are likely to be vulnerable or have violent tendencies; or have been making threats to kill; etc.

To identify if there are children at an address
There have been instances in the past where children have been injured during police raids on an address when officers were not aware children were resident in the property. On other occasions, children have been used by the occupants to prevent police entering an address. Officers may wish to ascertain if there are any children at the house and if so, the names and ages of children in order to establish if they are safely at school, in bed, etc.

To locate a missing person to ascertain their well-being
If a person goes missing the police have a responsibility to ensure their safety and well-being (i.e. not kidnapped, murdered, etc) and may require details of bank card transactions in order to ascertain if the card has been used and establish if it has been used by the individual or another party.

To progress enquiries into a Road Traffic Incident
There has been a single vehicle involved in an incident in which the vehicle has hit a tree and the sole occupant has been killed. One possible explanation is that the driver was making a telephone call at the time and lost control. Information may be sought from the phone company to see if a call was in progress at or around the time of the collision. This does not fit into categories 1 or 2 above for obvious reasons as there is no one to prosecute but all enquiries must be explored as part of the police investigation into the collision both for the Coroner and to provide closure for the relatives so 10 should be used.

To protect life or property
An anonymous caller reports that a named person she knows to be a childminder is neglecting the children in her care. The address of the child minder is not known so information is sought from Social Services to identify where she may live and so progress the investigation.
Another example may be where a handbag is found with some belongings which appear to belong to an elderly person. This includes a name and a spectacle case with details of an optician. The address or contact details of the elderly person is requested from the optician in order that a check can be carried out at the address to ensure that the person has not been the subject of a crime.

Other

There are many other examples and these few are intended as a guide to the way the categories in the table might be interpreted when completing the form. Staff should tick as many boxes that are relevant and be willing to explain to the organisation the nature of the investigation as far as is appropriate without jeopardising the investigation or subsequent proceedings.

RESTRICTED WHEN COMPLETE

Personal Data Request Form

To (*name and position if known*).....

Organisation & Address .....

.....

This request for personal data and other information is made under the powers invested in me as a constable of the Constabulary Police by the Police Act 1996 (section 30(1) which gives constables all the powers and privileges of a constable throughout England and Wales and Section 30(5) defines powers as powers under any enactment when ever passed or made). These powers include the investigation and detection of crime, apprehension and prosecution of offenders, protection of life and property and maintenance of law and order. Under the Police Reform Act 2002, the Chief Constable can delegate certain powers to police staff.

The personal data I require relates to the following individual(s):
(Include identifying details of the person where known, such as name, address and date of birth)

.....

.....

.....

I have the following information to assist you in locating the personal data and other information:
(Include further details, where available, to assist locating the information sought)

.....

.....

.....

I require the following personal data and other information:
(Describe the information sought)

.....

.....

.....

.....

.....

.....

I require the personal data and other information to assist with my enquiries into:
(Describe the subject of those enquiries as far as is possible without prejudicing them)

.....

.....

.....

.....

.....

.....

.....

RESTRICTED WHEN COMPLETE

I confirm the personal data and other information is required for the following purpose(s):
(Tick the relevant box(es) and complete the other row where necessary)

Purpose	Legal Basis	Tick
For the prevention, investigation and detection of crime	Police Acts, Common law	
For the apprehension and prosecution of offenders	Police Acts, Common law	
To confirm or corroborate information for intelligence purposes	Police Acts, Common law	
To put before a court to obtain a search warrant	Police Acts, Common law	
To prepare a file for the Coroner's court	On request of the Coroner	
To further a money laundering or confiscation investigation	Proceeds of Crime Act 2002	
To risk assess the address to safeguard the health and safety of any emergency personnel attending	Police Acts, Health & Safety, Common law	
To identify if there are children at the address to negate any harm caused by police action	Children Act 2004	
To locate a missing person to ascertain their well being	Police Acts, Common law	
To progress enquiries into a Road Traffic Incident	Police Acts, Common law	
To protect life or property	Police Acts, Common law	
Other (please specify)		

I request that the personal data and other information should be provided to the police in the following manner:
(Having considered factors such as the protective marking indicate how the information should be provided to the police, e.g. in person, by post, by fax, by email etc.)

.....

.....

.....

.....

The Data Protection Act 1998 defines personal data as data which is biographical in nature, has the applicant as its focus and/or affects the data subject's privacy in his or her personal, professional or business life. Under the Data Protection Act 1998, disclosure of personal data:-

- For the prevention and detection of crime or the apprehension or prosecution of offenders is permitted under s29(3)
- Required by or under any enactment, by any rule of law or by order of the court is permitted under s 35(1) (including the Health and Safety Act)
- For the purpose of, or in connection with, any legal proceedings is permitted by s35(2) (a)

Where no data protection exemption applies, consideration should be given to the first principle issue of fairness. Where the rights and freedoms or the welfare of an individual is in doubt such as in enquiries 8 and 9 above, a harm test should be applied. It is highly unlikely disclosure would be unfair in these circumstances.

Human Rights Act 1998 Article 8 – right to privacy. This request is consistent with Article 8(2) prevention of disorder or crime.

(To be completed by the officer requesting the personal data and other information – tick appropriate box(es))
I confirm that:

☐ this information will be used in connection with this enquiry and held and used only as long as this is required for policing purposes and any subsequent criminal justice proceedings.

☐ if this personal data is not disclosed it will prejudice the prevention or detection of crime or the apprehension or prosecution of offenders.

☐ if this personal data is not disclosed it will prejudice the purpose indicated overleaf.

Signed ..... Collar No ..... Date .....

Print Name..... Post .....

RESTRICTED WHEN COMPLETE

BCU/Area/Dept address.....

Phone .....Fax..... Email .....

If the nature of the enquiries is specified above this form must be countersigned by a Sergeant or Supervisor, if the investigation is such that no explanation can be given, this form will be countersigned by a Superintendent.

Signed..... Collar No..... Date.....

Print Name .....Post.....

This section to be completed by the recipient of request for personal data and information

Response

Please reply to all requests so that we know they have all been considered and to help prevent duplication.

As part of your decision making process, please take into account the requirements upon you/ your organisation in relation to the request, for example the Crime and Disorder Act 1998, (any person or organisation has a power to provide information to a relevant authority in order to achieve a crime and disorder objective), the Local Government Act, Children Acts 1989 and 2004, and other legislation relevant to your organisation

Signature.....Date .....

Name.....Position .....

Organisation & Dept .....

.....

.....

The information requested above has been approved for disclosure and is attached*

The information requested above has not been approved for disclosure*

**Delete as applicable*

Please explain why you have decided not to disclose the information so that we know whether you need additional information or for us consider presenting to the Court to obtain a Disclosure Order:

.....

.....

.....

.....

.....

.....

.....

.....

If there is insufficient room please continue on an additional sheet(s).

The subject of the request should not be given any indication that this request has been made prior to consultation with the requesting officer. If your organisation subsequently receives a request for a copy of this document (e.g. under the Data Protection Act or Freedom of Information Act) for this information, please contact the Force DP or FOI Officer.

Appendix G: Data Protection/Information System Operating Rules Template

This template may be used to create Data Protection or Information System Operating Rules, with type highlighted in blue replaced by appropriate content and other type amended according to Force needs.

Data Protection/Information System Operating Rules: [Name of Information System]

1. Introduction

These Operating Rules have been produced in accordance with the Force's [name of relevant] Policy.

They describe how the [Name of Information System] will be operated to ensure compliance with the requirements of:

Data Protection Act 1998;
Freedom of Information Act 2000;
MoPI CoP;
National Data Quality Standards;
Records Management Standards BS ISO 15489;
ACPO Data Protection & FOI Manuals of Guidance;
ACPO Information Systems Community Security Policy.

They set out standards, policies and procedures designed to ensure that considerations such as Data Protection Act compliance, disclosure or information sharing, data quality, review retention and disposal, training, access, storage, change control, and security and other protective measures are considered during the development and operation of the information system.

The will be managed by, or on behalf of, the Information System Owner, [Name of postholder, postholder title with overall responsibility for the Information System].

2. Summary

Name of Information System:	[Information System name]
Information System Owner:	[Name of postholder, postholder title and contact details formally nominated as such]
Information System Custodian (where applicable):	[Name of postholder(s), postholder title and contact details nominated as such by the Information System Owner]
Location of System:	[The location(s) where the system is used]
Purpose of the Information System:	[Description of the purpose(s) of the system]
Information Involved:	[Description of information handled by the system]
Operations:	[Description of the ways that the information is handled by the system – remember 'system' is likely to consist of more than simply an IT system, but will involved associated handling of information outside of the IT system. Link to Force Policy, Force Forms etc. where applicable]
Applicable Standards	[List of standards that apply to the system e.g. must comply with Home Office Counting Rules or National Data Quality Standards]
Version Control:	[Version number and date of production/revision of the Data Protection/Information System Operating Rules]

3. Responsibilities and Governance

The following summarises the roles of various individuals in respect of the information system.

Deputy Chief Constable, Chief Information Officer and Chief Constable

[Description of responsibility – something like: The Deputy Chief Constable, through the Chief Information Officer both supports and oversees Information Management matters, ensuring that relevant police policies, procedures and guidelines reflect the requirements of associated legislation and standards. The Chief Constable is legally responsible for the Force's compliance with the Data Protection Act 1998.]

Head of Information Management

[Description of responsibility – something like: The Head of Information Management oversees a team which provides compliance guidance to the Information System Owner, authorised users and any other person as required, and will instigate compliance testing as described at 4.7 below.]

Information System Owner and Information System Custodian

The Information System Owner (listed under 2 above) has overall managerial responsibility for the information system.

Under [name of relevant policy] the Information System Owner is required to ensure that Information System Operating Rules are completed describing how their information system will be used and managed.

For the purposes of practicality Information System Owners may nominate and oversee 'Information System Custodians' who actively manage many of the system ownership tasks on their behalf (though the Information System Owner will retain responsibility for the information system). Certain critical systems will have dedicated Information System Custodians.

Authorised Users

[Description of those persons authorised to use the system, their required level of vetting, and training standards - this may include non-police staff such as authorised contractors and volunteers, as well as managers, supervisors, system administrators and so on, who carry out 'day-to-day' activities on behalf of the Information System Owner. The table below is an example of how access types and eligible user criteria can be summarised.]

Access Type	Eligible User Criteria
Normal Access (Read only)	Individual is a Police employee, whose role, either temporary or permanent, requires the ability to access, create and amend data on the Information System.
Full Access (Input and Read)	Individual is a Police employee, whose role, either temporary or permanent, requires the ability to access, create and amend data on the Information System. The user will also be able to validate and reject crime reports.
IT Administration	Individual is a Police employee, whose role within the I.T. Department, either temporary or permanent, requires the ability to access the Information System for system administration purposes only.

The section will also describe the process by which users are nominated and the functionality of the various levels of access granted to each user type, and revocation procedures.

For practicality and audit purposes it is recommended that Information System Owners develop application forms which are completed for each new potential user of the Information System. These can record the nominal details of the user, confirm the appropriate level of access, confirm how long

access is required, and provide a space for approval or rejection by the system owner. The forms can be used as a prompt for IT Administrators to set up access.

This section should include a reminder that access to information on the system is permitted only for legitimate policing purposes and allowed only to those persons in the course of their agreed official duties and on a 'need-to-know' basis.

Where non-employees are likely to have access to or use personal information system within the information system on behalf of Police the Data Protection Act 1998 imposes special requirements relating to 'Data Processors'. Further advice on these can be obtained from the Data Protection Officer.]

[Add in any other user types]

4. Standards

Collection of Information

[Description of how information will be collected onto the system – where personal information is collected it should describe how the fair and lawful elements of the Data Protection Act 1998 are achieved (further guidance may be obtained from the Data Protection Officer) and should link to relevant policy where appropriate.]

Data Quality

[Description of how information on the system will be held in compliance with Force standards on Data Quality - it should link to relevant Policy where appropriate (further guidance may be obtained from the Force's Data Quality lead).

This should also describe how personal information on the system will be kept up-to-date where necessary, will be accurate, adequate, relevant and not excessive. Further guidance on this can be found in chapter 5 of the ACPO Data Protection Manual of Guidance or from the Data Protection Officer.]

Records Management

[Description of how information on the system will be held in compliance with the Records Management Policy - it should link to relevant Policy where appropriate. Reference should be made of procedures to archive hard copy records to the Force's archival store. (Further guidance may be obtained from the Records Manager or equivalent)]

Review, Retention and Deletion of Personal Data

[Description of how information on the system will be reviewed, retained or disposed when no longer required - it should link to relevant policy where appropriate, such as the force retention schedule (further advice may be obtained from the Records Manager or equivalent)]

Security and Protective Measures

[Description of technical and organisational measures established against unauthorised or unlawful use of information and against accidental loss or destruction of, or damage to, information within the information system.

There can be no standard set of security measures which collectively achieve this as the appropriate measures will depend on the circumstances.

The Information System Owner will need to adopt a risk-based approach to determining what measures are appropriate – effectively a 'balancing act' – and need to consider management and organisational measures as well as technical ones. Further guidance may be found in the ACPO Community Security

Policy (CSP).

Information System Owners may use standard risk assessment and risk management techniques which involve identifying potential threats to the system, the vulnerability of the system to those threats and the necessary counter-measures to put in place to reduce and manage the risk.

The police service, through the adoption of the Government Protective Marking Scheme (GPMS), provides a mechanism for valuing information assets and affording necessary levels of protection to that information.

The more 'sensitive' the information then the greater the protective measures that will need to be put in place. Within policing this is likely to mean that information, for example, relating to confidential human intelligence resources is likely to be afforded far greater protection than an intranet directory of police headquarters' staff work telephone numbers. In many cases, a simple consideration of these matters will be sufficient. On the other hand, there are well-established methodologies which will assist police forces in assessing and managing the security risks to theirs systems which can be found in the ACPO CSP.

Where associated Risk Management Accreditation Document Sets (RMADSs) exist they should also be referenced and in themselves may be sufficient for this section.

Further advice on completing this section may be obtained from the Information Security Officer.]

Transfers outside the European Economic Area

In the (unlikely) event that personal information within the system is to be transferred beyond the European Economic Area the Data Protection Officer will be contacted for advice on the special considerations that this would invoke. These are documented in Chapter 9 of the ACPO Data Protection Manual of Guidance.

Monitoring and Inspection

[Description of any monitoring or validation process adopted to ensure that the information system is being used appropriately. The expectation is that the more sensitive the system, the greater the level of monitoring and inspection of users.

Where the information system is likely to be subject of a Data Protection compliance audit, details of the audit methodology should be described (or referred to if in a different document) from here. A similar approach should be adopted regarding Data Quality audits.

It should also describe how allegations of misuse of the system potentially leading to criminal offences will be handled – with links to relevant policy where appropriate.]

Disclosure

[Description of how disclosure of information from the system is managed. It should link to relevant policy, memoranda of understanding, information sharing agreements, decision-making models, and disclosure tables such as below which may be useful in certain circumstances.

Recipient	Reason / Circumstances	Protocol/ Contract	Authorisation Required
example: All other law enforcement agencies at level 1, 2 and 3.	Sharing of intelligence in accordance with the National Intelligence Model.		Area/Force Intelligence Managers

Other agencies connected with the Tactical Tasking and Co-ordination process as required.	Sharing of intelligence in accordance with the National Intelligence Model.		Area/Force Intelligence Managers

Further guidance on disclosure can be obtained found in Chapter 11 of the ACPO Data Protection Manual of Guidance].

Information Requests

Requests for information held on the system made under the Freedom of Information Act 2000, Data Protection Act 1998, required by Court Order, and for civil litigation purposes will be forwarded to the Data Protection Officer at Police HQ for action and handling in accordance with Policy [name of policy].

[Add in any additional local arrangements]

Information Rights and Complaints Resolution

Under the Data Protection Act 1998 individuals have various rights relating to their personal information held on the information system. Those rights include:

- Right to prevent processing likely to cause damage or distress;
- Rights in relation to automated decision taking;
- Right to take action for compensation if the individual suffers damage by any contravention of the Act by [Force Name];
- Right to take action to rectify, block, erase or destroy inaccurate data.

Generally these rights will be enacted by the individual writing to the Force, and any such correspondence will be forwarded as soon as possible upon receipt to the Data Protection Officer to co-ordinate the response in accordance with the ACPO Data Protection Manual of Guidance.

Where the action relates to a claim for compensation that will be forwarded to the [Legal Services Department] who will liaise, where appropriate, with the Data Protection Officer.

Any person wishing to dispute the processing of personal information system will be required to put their case in writing to the Data Protection Officer who will progress the matter in accordance with the ACPO Data Protection Manual of Guidance.

[Add in any additional local arrangements.]

Change Control

[Description of how changes to the system made will be managed – this should link to relevant policy where appropriate.]

5. Guidelines for Users

[Where they exist, details of additional guidance for users should be listed.]

6. Review

The Information System Owner will ensure that these Operating Rules are reviewed on at least an annual basis.

Appendix H: Version Control

This appendix details any *significant* amendments to the ACPO Data Protection Manual of Guidance Part 1.1: Standards.

Date	Version	Place	Comments
10th October 2006	1.0	General	Version 1.0 issued to all DPOs via email and placed upon Genesis. Subsequently published on the ACPO Intranet.
12th March 2007	1.1	Appendix G	Version Control Appendix added.
12th March 2007	1.1	General	Minor typographic errors corrected, font size increased to aid those with impaired vision.
12th March 2007	1.1	2.3 Processing of personal data by the police	Final paragraph appended to clarify there is a limited right of access to personal data under the FOI Act.
12th March 2007	1.1	3.2.5.1 Schedule 3: Introduction and 3.2.5.6 'Unlawful act etc.'	Paragraph 1 of SI 2000/417 added as a likely schedule 3 condition for processing. The inclusion of the new associated section 3.2.5.7 has led to the former 3.2.5.6 'Conferred on a Constable' being renumbered as 3.2.5.7.
12th March 2007	1.1	3.6 Standards	New standard added, derived from 3.4 (disputes/complaints).
12th March 2007	1.1	5.6.2 Identification - Footnote	Amended to indicate that height may not always be required when a subject access application is from a person known to the police force.
12th March 2007	1.1	5.6.2 Identification - Footnote	Footnote added to refer to HMSO Guidance on copying various official documents.
12th March 2007	1.1	5.15 Standards	New standard added, derived from 5.6 (unsatisfactory applications).
12th March 2007	1.1	7.9 Standards	New standard added, derived from 7.2 (consultation with data protection officer).
12th March 2007	1.1	7.9 Standards	New standard added, derived from 7.3 (vetting).
12th March 2007	1.1	7.9 Standards	New standard added, derived from 7.6 (amendment of data protection operating rules).
12th March 2007	1.1	9.3.2 and 9.7 Standards	Requirement to ensure the data protection officer is 'kept in the loop' (regarding the progress of any criminal investigation re police personal data) is reinforced.
12th March 2007	1.1	9.5 Related Offences	Addition of Fraud Act 2006.
12th March 2007	1.1	9.7 Standards	New standard added, derived from 9.2 (breaches of principles).
12th March 2007	1.1	9.7 Standards	New standard added, derived from 9.3.2-9.6 (S55 offences).
12th March 2007	1.1	10.7 A to Z Disclosure Reference.	Removal of final sentence regarding resourcing to produce the A to Z Disclosure Reference.
26th February 2009	2.0	1.2.1 Chief Officer – Data Controller	Examples of 'joint' and 'in common' data controllers added following advice from the Information Commissioner in letter dated 26th April 2007.
26th February 2009	2.0	1.7.2 Portfolio Group Terms of Reference and Structure	Terms of reference removed. These are now a standalone document retained by the ACPO ranked officer maintaining the portfolio.

26th February 2009	2.0	3.2.3.4 The Police's use of 'Fair Processing Notices'	Reference made to Essex Police's fair processing notice as one that may be adopted or adapted by other forces.
26th February 2009	2.0	3.2.4.5 Schedule 2: 'Public Functions'	Commentary added regarding 'administration of justice'.
26th February 2009	2.0	5.14	New section recommending forces obtain in writing formal withdrawal of subject access applications when that is the case – inserted following a recent ICO view regarding a police force that had not obtained confirmation of the withdrawal in writing. Previous sections 5.14 to 5.15 now renumbered 5.15 and 5.16.
26th February 2009	2.0	5.5 National and Local Applications	Redrafted for greater clarity. Reference now made to 'Editing Guidance'. Reference made to the forthcoming transfer of National applications from NIS to ACRO.
26th February 2009	2.0	5.7.3.1 Section 29(1): Crime and Taxation	Useful reference to R (Lord) v Secretary of State for the Home Department added.
26th February 2009	2.0	Subject Access Form	Subject access form amended to reflect access to firearms database via PNC and to assist data input by NIS staff.
26th February 2009	2.0	9.2.1 Section 55	New defence derived from section 78 of the Criminal Justice and Immigration Act 2008 added. New power for the Secretary of State to make an order altering the maximum penalty for an offence under section 55 added - derived from section 77 of the Criminal Justice and Immigration Act 2008
26th February 2009	2.0	10.6 Disclosures required by law or made in connection with legal proceedings etc. (section 35)	Entire 10.6 content substantially expanded and two new standards added at 10.8
26th February 2009	2.0	11 Powers of the Information Commissioner	New section added
26th February 2009	2.0	Appendix C: Template and Guidance for a Data Processing Agreement	Entire section revised
25th February 2010	3.0	4 Privacy Impact Assessments	New chapter inserted. Former chapters 4 to 10 now become 5 to 11
25th February 2010	3.0	6.10 Enforced Subject Access	New reference added to Access Northern Ireland
25th February 2010	3.0	8.6 Data Protection/Information System Operating Rules	Updated to refer to new Appendix G
25th February 2010	3.0	Appendix G: Data Protection/Information System Operating Rules Template	New Appendix G inserted. Displaced former Appendix G now becomes new Appendix H