Witness:	Jerry Kirkby
Statement No:	2
Exhibits Referred to:	JK/1, JK/2, JK/3, JK/4, JK/5, JK/6
Date Statement Made:	21 March 2012

The Leveson Inquiry into the Culture Practices and Ethics of the Press

Witness: Jerry Kirkby

Occupation: Assistant Chief Constable

Address: Surrey Police, Mount Browne

1. Further to my statement dated 2 March 2012, I have been asked to provide this statement for the purpose of assisting the Leveson Inquiry. In preparing this statement I have sought to address all questions asked of Surrey Police in the Notice served pursuant to s.21(2) of the Inquiries Act 2005. Given the specific nature of some of the questions asked, the details were not within my knowledge until I caused inquiries to be made by various business areas within the Force to collate this response.

(1) Who you are and a brief summary of your career history.

2. I am currently the Assistant Chief Constable of Surrey Police and have held this position since 2008.

3. I began my policing service with Surrey Police in 1983 before transferring to the Metropolitan Police in 1998 on promotion to Chief Inspector.

4. Whilst within the Metropolitan Police I served at Wandsworth, Southwark and Sutton, also completing a 6 month posting to the Directorate of Public Affairs (DPA) as head of Internal Communications and Publicity.

5. In 2001, I returned to Surrey Police on promotion to Superintendent and took up the role of Head of Operations at North West Surrey. A year later I became Divisional Commander (Chief Superintendent rank) for West Surrey, covering Guildford and Waverley Boroughs.

6. Between 2005 to 2008, I was seconded to ACPO and then the National Policing Improvement Agency as the National Programme Director for the implementation of Neighbourhood Policing Programme before returning to Surrey Police as Assistant Chief Constable.

(2) Please identify the databases, owned and operated by Surrey Police, that hold personal/private information relating to individuals, for example the local intelligence database. In respect of each database please explain (i) what broad categories of information are held on it; and (ii) who has access to it and for what purposes.

7. Surrey Police uses 71 applications that hold personal information; some of these systems only hold information about officers and staff (e.g. our internal HR system). A number of systems utilised and supplemented by Surrey Police are nationally owned and maintained including the Police National Database (PNC), the Violent Sex Offenders Register (ViSOR) and the National Special Branch Intelligence System (NSBIS). I do not intend to comment upon these systems in this statement save where specifically asked, however I will provide further information should the Inquiry require it.

8. The 'Surrey Applications Impact Questionnaire Final' (Exhibit **JK/1**) details the 71 applications referred to. All of these systems have associated structured databases.

9. I have been advised that, bearing in mind the time constraints, the Inquiry would be best assisted by me focussing on those databases holding information on crimes and on members of the public rather than dealing with each of the 71 databases. Many of these databases store internal information such as finance, human resources and shift patterns. Others deal with specialist investigative areas such as suspect footwear intelligence linked to crime scenes, or provide details of fingerprints for those who enter Surrey Police custody centres.

10. Should further information be required on any of those databases that I have not focused on, these details will be provided on request.

11. Listed below are the main databases that store crime related information such as crime reports made by the public and the linked investigation into these crimes, as well as intelligence held on suspects. This list also includes specialist databases that are held in relation to storing data for instance on national security and murder/major crime investigations.

12. **The Crime Information System (CIS)** stores details of all crimes reported to the police by the public. It stores all details of the investigation including victims, witnesses and where arrested, any suspect custody details. This system also acts as a parallel intelligence database containing all levels of security intelligence except those relating to national security. This system is used and accessed by the majority of police officers and staff and varying levels of access are allocated depending on the individual role and security vetting level. Staff in specific specialist roles have full access to the system.

13. During the course of 2012 CIS will be superseded by a newly developed and bespoke database called Siren.

14. **ABM Pegasus** is a central intelligence administration system used for creation, input and management of intelligence prior to its sanatisation and inclusion on CIS. This database contains details of informants, submitting staff and any subsequent risk assessments. All Police officers and staff within an operational policing role have access to submit intelligence, however only specific roles with enhanced levels of security vetting have access to administer and search the system any further.

15. **IBase** is analytical based software that draws information and intelligence from all Surrey Police systems enabling the data to be displayed, analysed and used in conjunction with each other. These systems include CIS, Automatic Number Plate Reading system (ANPR) and data from telephone calls to the police from the public and the police response to these (ICAD). This system is predominantly operated by intelligence analysts with enhanced security vetting.

16. **The Home Office Large Major Enquiry System (Holmes)** is a system to record and manage the investigation of major crimes. It records, *inter alia*, actions that have been completed by the investigation team as well as witnesses and suspect data and documents. This system is predominantly used by the Major Crime Team.

17. **The Central Logging of Intelligence Operations (CLIO)** system is used to record and manage "crimes in action" such as kidnap. Access is provided to those working in this specialist fields such as intelligence and serious crime investigations.

18. **Intergraph Computer Aided Dispatch (ICAD)** is the system that records the detail of calls made from the public and the response to these and/or the deployment of Surrey Police resources to an incident.

Input access is limited to those specifically trained due to their job role, for instance those working in intelligence units or within the control room. The majority of Surrey Police staff can perform basic searches of this database to assist with crime investigations. Specific incidents can have access restricted if required.

19. **The Automatic Number Plate Recognition (ANPR)** database records data on vehicles that activate cameras on roads in Surrey. This information is then cross checked against data held on the Police National Computer (PNC) to identify if they have been used in crime or have intelligence markers placed upon them. Access is limited to those working in specialist roles, including those dedicated to policing Surrey's strategic roads network and supporting intelligence and investigation departments.

(3)How does information get placed on those databases? Who decides whether the information should be inputted?

20. Surrey Police follows the Management of Police Information (MOPI) and National Intelligence Model (NIM) guidelines on storing and retaining information that is for a policing purpose. This covers collecting, recording, evaluating, analysing, sharing, reviewing and retention of material held by the police. Guidance for staff is available on the force intranet including a flow chart of 'The Information Life Cycle' (Exhibit **JK/2**). Managed learning environment packages are also provided to staff via the National Centre for Applied Learning Technologies (NCALT).

21. **CIS** - Data is entered by staff in accordance to their specific role and function within the organisation. An example of this would be an officer attending the scene of a burglary. Those officers initially attending would obtain details and record the initial report, intelligence staff would research the crime and add any further intelligence to identify a

suspect, and custody staff would record the details of any offender subsequently identified and arrested for the offence. Guidelines such as the National Crime Recording Standards determine what is added to the database.

22. **ABM Pegasus** – Trained data processing staff are employed to create, assess and input intelligence. All police officers and operational police staff are encouraged as part of their role to submit intelligence. The data processing staff ensure the quality, grading and value of this intelligence prior to recording it on CIS.

23. **IBase** – This system is an analytical based tool which draws information from other databases and therefore does not require the inputting of data.

24. **HOLMES** - Designated staff can input data onto Holmes and access levels are set during a specific investigation dependant on what role and individual is completing, for instance indexers add information obtained in categories such as names, addresses, vehicles. Trained receivers decide what is recorded on the database following the Senior Invesigating Officer (SIO) strategy for the investigation.

25. **CLIO** - Information is added by those working on a specific investigation from the dedicated roles of surveillance, intelligence and negotiation and those in key management roles such as the Senior Investigating Officer. All of those working in the operations room can add data to CLIO, which operates so that real time updates from all the different roles are recorded and logged against the time of the update. This allows the Senior Investigating Officer to have all information available at a particular time in one place to aid his/her decision making.

26. **ICAD** - Information is added by those who handle the calls from the public or manage the deployment of police resources. When a member

of the public telephones the police, the call handler will take the details of that person, the address and a summary of the reason for the call. They will then decide and record the police response to this information. When the police attend the incident any updates provided from the scene are normally provided by radio and updated on this specific incident, which is designated a unique reference number. This allows the police to identify repeat victims from their names and addresses by searches that call handlers and intelligence officers can complete. Location markers can be added to a name or address to flag repeat victims of officer safety information; such additions require a higher level of approval.

27. **ANPR** – Vehicle information comes via PNC in the case of stolen vehicles or national crime markers. Intelligence held on either the vehicle or suspected users can be added by individual police forces via back office intelligence and investigation staff based on its suitability.

(4) How do users access the databases?

28. To access any application (either locally or nationally hosted) users must first logon to the Surrey Police network using a username and password that identifies the individual. Users are forced to change passwords periodically and strong password rules are in place to ensure an appropriate level of complexity.

29. Once logged on to the network, access to individual applications vary depending on the individual's security access and necessity to have access to the information contained within. Broadly this will either be supported through a security group on the network which works with the credentials the user has already provided to logon or through a separate username and password for the specific application. Password rules vary with every application dependent on the individual's role and requirements.

30. Once the user has accessed the Surrey Police computer network via an individual username and password, they are then (with the exception of ABM Pegasus and iBase) required to enter that specific database by a further individual password.

31. ABM Pegasus automatically recognises users after they log onto the Surrey Police network. Further user names and passwords are required for those staff with permission to administer or search the system.

32. iBase user identification is automatically recognised to give initial access followed by the requirement for a further personal log-on.

(5) How is access to those databases restricted and controlled? The Inquiry is interested in both technical and non-technical measures (such as instructions to users).

33. From a technical perspective, access is controlled either through the management of user accounts on individual applications or through managing 'security groups' within the 'Active Directory' (the Microsoft technology used to manage authentication of users on to the network). In some cases, managing access is delegated to business owners of systems while in other cases it is facilitated through a request to the Shared Business Service Centre and carried out by Support Services staff. In all cases authorisation is required from business owners of systems (and is usually based on completion of appropriate training – again this varies from system to system).

See 'Surrey Applications Impact Questionnaire Final' (Exhibit **JK/1**) for a brief summary of key systems and their authentication method.

34. **CIS Intelligence** – Access is given according to 4 grades:

1) No access to intelligence
2) F – general operational staff
3) B – intelligence staff and specific investigation teams
4) A – selected intelligence staff.

The Head of Intelligence authorises access to B and A level intelligence, which is given to specific named individuals based upon their role. Training is given to users regarding access, relevant legislation, policy, guidance and the consequences of misuse.

35. **ABM Pegasus** – All staff are able to access this in order to submit intelligence. Only trained intelligence processing staff and intelligence supervisors have a higher level of access in order to process, sanitise and search the original intelligence submission. This is controlled by role type and supported by role specific training.

36. **iBase** – Access is role based and supported by role specific training. Compliance with all appropriate legislation, guidance, policy and practice is assessed via the Intelligence Analysis NVQ which is the qualification analysts have to obtain before achieving "higher" status.

37. **HOLMES** – Access is role based to those working on major crime investigations mainly on the Major Crime Team. Further restrictions ensure officers and police staff only have access to those operations they are involved in – rather than staff having access to all operations. Access is provided to individuals by the Holmes Support Team who manage the database and provide training to national standards and conventions.

38. **CLIO** – Access and training is given by Holmes Support Team to only those designated to work on a specific operation as determined by the SIO.

39. **ICAD** – Input access is role based. All Surrey Police staff can access

a view/search facility for specific incidents. Specific incidents can be restricted by supervisors within the Control Room should information contained within the log be deemed as sensitive.

40. **ANPR** – View/search access is role based and information can only be obtained for a three month period unless supported by an application to a Superintendent. Access and training is provided by the ANPR team and is overseen by the ANPR manager. Inputting access is limited to a number of individuals working within the department.

(6) What systems and/or measures are in place to ensure that information held on the databases is not misused? The Inquiry is interested in both technical and nontechnical measures.

41. Prior to being given access to both internally and externally hosted systems, all users receive training regarding what amounts to misuse and what the consequences of misuse would be. Additionally there is a Force policy owned by the Professional Standards Department regarding the acceptable use of Surrey Police computer systems (Exhibit **JK/3**). This is accessible by all Surrey Police staff under policies and procedures on the intranet. Reminders of acceptable conduct are periodically circulated to all staff by Routine Orders published on behalf of the Deputy Chief Constable and circulated weekly. It is a standing order that it is the responsibility of all staff to view this circulation.

42. Access to Surrey Police applications or databases e.g. CIS and ICAD, or National applications e.g. PNC or ViSOR is granted for official police purposes only. Personal browsing or use of these applications or the information contained within them is not permitted under any circumstances. This is detailed in the policy and procedures detailing acceptable computer use which can be accessed by all staff under

policies and procedures on the Intranet.

43. Computer systems may only be accessed by authorised users. All Surrey Police computer systems are capable of either automated electronic monitoring or manual monitoring, scrutiny or intervention.

44. Authorised users are regarded as those who have a valid Force Identification Number (FIN) and, where applicable, have had the appropriate training to access Surrey Police systems or applications. The computer procedure states that managers are responsible for conducting dip checks on those they are responsible for and also details the relevance and application of the Data Protection Act.

45. Additional guidelines are in place to limit the use of memory sticks and similar external storage devices. A written report is required to justify the use of devices that can be used to transfer data. On the rare occasions that these requests are granted memory sticks which require bio metrics to access the stored data are issued.

46. Guidance is provided regarding the changing of passwords which must be changed regularly when prompted by the computer system or if the password has been compromised. Passwords must be at least 8 characters long and cannot be re-used for a 12 password cycle. Once a password has been changed it must remain for a minimum of 2 days.

47. The majority of databases owned, administered or used by Surrey Police allow three wrong password attempts before the user is locked out.

48. Databases such as HOLMES have warning statements on the front screen informing users that unauthorised access is prohibited and that unlawful disclosure of information is an offence under the Data Protection Act 1998. It also states that illegal use is an offence under

the Computer Misuse at 1990. CIS states on the front screen that all data on this system is subject to the Data Protection Act 1998 as amended.

(7) Are individual users subject to any vetting procedures or security checks? If so, please give details. Is there a system in place for monitoring and reviewing the suitability of a person to have continued access to the databases? If so, please give details.

49. All individual users of the Surrey Police network and the applications included within it are subject to vetting procedures. Surrey Police complies with the vetting standards set out in the ACPO & ACPOS National Vetting Policy for the Police Community (August 2010). All users of our computer systems will be vetted to a baseline standard of 'Recruitment Vetting' as set out in this policy. Some users will have a higher level of vetting dependent upon their role and the confidentiality or sensitivity of the information they need to access, for example, IT System Administrators are all vetted to Security Check (SC) level due to the level of their access rights to information.

50. Individual users with a higher level of vetting (Management Vetting (MV), Security Check Vetting (SC) or Developed Vetting (DV)) are subject to an annual re-evaluation whereby their line manager assesses their continued suitability to hold that level of clearance for the purposes of their job role.

51. All employees / users are also required to notify the Vetting Team of any change in their personal circumstances that could affect their suitability to maintain their particular security clearance. On receipt of any such information the Vetting Team will conduct checks to establish the levels of risk and whether a person should their access rights reviewed.

52. If an employee is subject to a misconduct investigation a review will take place within the Professional Standards Department in order to determine the individual's continued suitability to access systems/information.

53. Vetting levels depend on the individual's specific role and databases they require access to fulfil their role. For instance, those working in the intelligence units which have the higher access to CIS and can access PNC, ANPR, ABM Pegasus and iBase have SC clearance.

54. Those working in major crime, serious crime and public protection/risk management are required to have a minimum level of MV vetting.

(8) Are any restrictions placed on an individual user's ability to access information held on the databases (whether by technical means or by way of instructions to the user)? For instance, do some users have greater access rights than others? If so, describe the levels of access and to whom they apply respectively.

55. Access rights within applications are used to restrict who sees what; these are typically based on either a functional restriction (allowing only certain users to see certain screens of fields or subsets of complete records) or a record restriction (only certain users have access to certain records).

56. Some applications also restrain access to specific end-user desktops or devices as an additional layer of protection. For instance, some HOLMES investigations can only be accessed on some enabled computers and only then if the correct user passwords are also used.

The 'Surrey Applications Impact Questionnaire Final' (Exhibit **JK/1**) provides a brief summary of key systems and their internal rights management methods.

(9) Are individual users permitted to browse the information to which they do have access without restriction? If not, what restrictions are in place and how are they communicated to individual users?

57. Users are not permitted freely to browse the information they may have access to. 'The Acceptable Use of the Surrey Police Computer Systems' Policy (Exhibit **JK/3**) and 'The Acceptable Use of Surrey Police Computers' procedure (Exhibit **JK/4**) state that personal browsing or use of applications or the information contained in them is not permitted under any circumstances and that access to systems is granted to authorised users for official police purposes only.

This is re-enforced by the 'Surrey Police Security Matters' handbook (Exhibit **JK/5**) which states:

"It must be understood that whilst you may be able to access a system this does not give you the right to access that system at any time other than for legitimate reasons. You must not disclose Surrey Police information to any person who does not have a legitimate reason to have that information. If you access any information held on a computer without authority, or if you use a computer for a purpose for which you have no authority (for example curiosity...) you are committing a criminal offence....... Surrey Police does not tolerate inappropriate use of any of its systems. Any apparent breach of the computer systems polices will be investigated and where appropriate disciplinary action will be taken up to and including dismissal."

58. CIS is the only database mentioned which can be searched by the majority of Surrey Police staff, however the 'The Acceptable Use of the Surrey Police Computer Systems' policy (Exhibit **JK/3**) states:

"Access to Surrey Police applications or databases e.g. CIS and ICAD, or National applications e.g. PNC or ViSOR is granted for official police purposes only. Personal browsing or use of these applications or the information contained in them is not permitted under any circumstances".

59. Searching on CIS can only be achieved within the security access levels individuals have been afforded. For instance, general staff cannot access higher level intelligence. Specific crime reports can be locked if required so that only nominated individuals can access them. Searching of the system is required by staff on a regular basis to identify linked crimes, possible suspects and intelligence to support warrants etc.

60. Other databases are restricted to those working on specific operations or working in specific specialised areas of business. In relation to ICAD and Visor it is important that nominated users can identify if police have previously attended a particular address and whether there is any linked intelligence. This means that access to these restricted individuals needs to be wide so that other risks to the organisation can be avoided, such as failing to identify repeat victims or potential suspects.

61. The Surrey Police 'Acceptable Use of the Surrey Police Computer Systems' policy (Exhibit **JK/3**) and the 'Acceptable Use of Surrey Police Computers' procedure (Exhibit **JK/4**) are available to all staff on the intranet and training courses also detail what is, and what is not acceptable. Surrey Police staff are aware that PSD can and do audit what has been accessed by individuals.

(10) What training is provided to individual users of the databases to ensure that they understand what is and what is not lawful/appropriate

use of the information held on the databases? Who is responsible for providing this training?

62. All employees receive information in relation to the Data Protection Act; and users should be aware of the need to protect and handle personal data in accordance with the provisions of the Data Protection Act 1998. This training is delivered through a combination of e-learning and classroom based training within Surrey Police.

63. Users of the primary intelligence databases operated by Surrey Police including the Crime Information System, HOLMES, Police National Computer and Police National Database are required to attend training before they may become authorised users. This includes training in what Surrey Police deems acceptable usage.

64. Training is primarily provided by the Force Learning and Development Team, IT Faculty in accordance with nationally or locally agreed standards appropriate to the system.

65. The 'Acceptable Use of Surrey Police Computer Systems' policy (Exhibit **JK/3**) and the 'Acceptable Use of Surrey Police Computers' procedure (Exhibit **JK/4**) state that personal browsing or use of applications or the information contained in them is not permitted under any circumstances and that access to systems is granted to authorised users for official police purposes only.

66. **CIS Intelligence** – General training (F level access) is delivered by the Force Learning & Development Faculty. Training for intelligence professionals is provided by the Intelligence Training Team and covers specifically legislation relevant to the role and information accessed.

67. **ABM Pegasus** – Training for intelligence professionals is provided by the Intelligence Training Team and covers specific legislation relevant to the role and information accessed.

68. **iBase** - Training for intelligence professionals is provided by the Intelligence Training Team and covers specifically legislation relevant to the role and information accessed.

69. **HOLMES** - Training is provided by the Holmes Support Team and varies in duration from two days to a month dependant on the role the person will be performing; this includes what is appropriate access.

(11) What systems and/or measures are in place to audit the use of the databases by individual users? Describe the system of auditing, if any, that is in place.

70. With regard to the Force main intelligence databases, a user's username/password is used to generate an audit trail for every auditable action they perform.

71. Auditing capabilities exist in the majority of applications. Typically these will record actions that users have taken within the application (e.g. records viewed, records updated). There is a variance in the capabilities and granularity of information each application offers depending on the facilities that vendors have written into their application; this is typically driven by business need (within the police service as a whole).

The 'Surrey Applications Impact Questionnaire Final' (Exhibit **JK/1**) provides a brief summary of key systems and their internal auditing capability.

(12) What systems and/or measures are in place (i) to prevent; (ii) to detect and (iii) to deter individual users of the databases from unlawfully disclosing information?

72. Individual use of some Surrey Police systems are monitored and can be audited. With regard to the primary Force intelligence databases, a user's username is used to generate an audit trail for every auditable action performed. Users receive training with regard to the Data Protection Act so they are aware of their obligations in relation to the handling of personal data. All staff sign the Official Secrets Act. Training and supervision also prevent misuse of Surrey Police databases. Additionally on some investigations confidentiality agreements are signed by those working on them.

73. The detection of incidents involving the misuse or unlawful disclosure of information is very often due to the receipt of intelligence, either via the 5x5x5 system or via the Anonymous Reporting system, both of which are open for everyone in the force to use. On receipt of any intelligence or allegation of computer misuse or unlawful disclosure, the Professional Standards Department will instigate enquiries. PSD will investigate all issues of unlawful disclosure of information.

74. Where investigations by PSD prove that information has been unlawfully accessed or disclosed the result, including the sanction following any disciplinary proceedings, is published on the force Routine Orders under the category misconduct/disciplinary hearings.

75. Databases carry warning pages and statements as set out at paragraph 48 are displayed.

76. PSD provides training inputs to all members of staff during their induction process. They also regularly deliver training inputs on courses such as CID courses, leadership training, response and

neighbourhood officers training days. The training gives examples of recent misconduct cases in the police service which focus on the misuse of computer systems.

77. All new staff are required to read and sign the 'Surrey Police Security Matters' handbook which clearly sets out individual responsibilities and references the policies in relation to the acceptable use of computers.

78. PSD does not conduct random checks on any computer systems but act on intelligence of misuse. They conduct regular audits as a result of their investigations.

79. As previously disclosed in paragraph 57, personal browsing or use of applications or the information contained in them is not permitted under any circumstances.

(13) Do you consider that the systems and/or measures referred to in question (12) above work effectively? What changes, if any, do you consider should be made to them?

80. Surrey Police completes a 'Force Information Risk Appetite Statement' (Exhibit **JK/6**). The statement enables people, particularly those involved in Information Risk Management, to take calculated risks when opportunities arise that will improve service delivery and, conversely, to identify when a more cautious approach should be taken to mitigate threats or risks in the handling of information. Each database has a level of risk calculated from a set matrix so that a strategy can be put in place to manage it to the level required.

81. In addition, the 'Force Information Risk Appetite Statement' assists in trying to embed a culture of information risk management and accountability. The risk appetite statement for Surrey Police is set by the Senior Information Risk Officer (Deputy Chief Constable).

82. The 'Force Information Risk Appetite Statement' sets out the amount of risk, at a corporate level, the force is prepared to accept, tolerate or be exposed to at any point in time. The Risk Tolerance allows for variations in the amount of risk the force is prepared to accept for a particular project or business activity. It will take into consideration the political or operational imperatives driving the activity, and ask in the context of the particular activity whether there are certain categories of risk which the organisation may be more or less willing to accept.

Tolerance levels for risk take into account and include the following:

- In the context of this system are we averse to certain types of incidents, e.g. interception by criminal groups?

- Are we less concerned about certain types of risks, e.g. unauthorised access by third party staff?

- Are there particular political or operational imperatives relating to the system?

- Have incidents in the past indicated a tendency for risks to this information to be exploited?

- If we are handling data owned by partners or third parties, what is their Appetite / Tolerance for information risk associated with this system? What rules do they have for handling that information?

- If we are passing data to partners or third parties, do we trust their handling of our sensitive data, and are we sensitive to any risks that they pose to the information?

- Are we more or less willing to pay to mitigate risk?

- Because in the context of this system, the risks of disclosure, confidentiality, integrity of the information are NOT deemed to have serious impacts?

- Budgetary pressures have become the norm; this is not regarded as a reason to apply a higher Risk Tolerance for a system. However, it may influence the decision not to spend on the risk mitigation options proposed in a Risk Balance case.

83. The force has articulated its local Information Risk Appetite as 'Open'. This means that the force is willing to consider all options and choose the one that is most likely to result in successful delivery while also providing an acceptable level of business benefit. This risk appetite has been partly driven by fiscal pressures and also by the desire to make users more flexible and mobile through the use of technology.

84. The Information Risk Appetite for National Systems such as PNC is 'Cautious'. This means the force should have a preference for safe options that have a low degree of residual risk and may only have limited potential for business benefit.

85. The systems and measures outlined in the questions above are effective to a point; to the extent that the vast majority of application users in Surrey Police behave appropriately to ensure that the information entrusted to us is protected, they have been successful. However, despite these measures the force still has occasionally to deal with individuals who choose, for whatever reason, to step outside of force policy, or in the case of PNC, national guidelines.

86. Both the force Security Advisor and Senior Information Risk Officer (SIRO) (Deputy Chief Constable) are satisfied that the level of non-compliance with policy and procedure sits within our stated Force Information Risk Appetite and where national systems are concerned

that we comply with the standards laid down within the Codes of Connection.

(14) In the last 5 years:

a. How many suspected unlawful disclosures have there been of information held on the databases to the media and/or private detectives?

b. How many investigations have there been into those suspected unlawful disclosures of information? What was the outcome of those investigations?

87. A review of the PSD database has identified four complaints and one conduct matter recorded in relation to the disclosure of information to the media or private detectives between 14/03/07 and 13/03/12. These were:

- CO.110578 – Complaint that information was disclosed to the press in Scotland. This case remains ongoing and therefore no further detail can be disclosed at this stage.

- CO.090612 – Complaint received following the disclosure of information to journalists via a press release containing details of the complainant's wife's death. Investigation by PSD revealed that the press release had been authorised by the SIO and was therefore not an unlawful disclosure. This matter was locally resolved.

- CO.100016 – Complaint received stating that Surrey Police had disclosed information to the BBC about the complainant's sons' trial. Following the initial allegation by the complainant they refused to engage any further with PSD which resulted in a dispensation being granted by the IPCC.

- CO.110502 – Complaint that personal and case details were disclosed to the press. This matter is currently in sub judice.

- CM.11.0078 - This is a recorded conduct matter against a Surrey Officer who is suspected of disclosing information to the press. This matter is under investigation by Operation Elveden. The officer has been suspended and I have referred the matter to the IPCC.

88. There have been a total of 34 incidents of either inappropriate access or disclosure over the last 5 years within Surrey Police. Of these incidents, 16 have been dealt with as Misconduct with the remaining 18 as Gross Misconduct.

(15) Do you consider that the unlawful disclosure of information from the databases is a current problem? Please explain your answer.

89. Surrey Police Professional Standards Department regularly investigate allegations of computer misuse. The vast majority of investigations relate to misuse of CIS and tend to be staff looking at information held about family, friends or neighbours.

90. Given the relatively small number of allegations of unlawful disclosure of information from localised databases and the circumstances that accompany them, I do not believe that Surrey Police has a significant system access security issue. However, Surrey Police remain committed to information security and always strive for security excellence through procedural reform of technological advance.

(16) As regards the personal/private information held on the Police National Computer, what role does Surrey Police play in preventing, detecting and deterring its personnel (both police officers and civilian

staff) from unlawfully disclosing such information? Please describe the systems and/or measures in place (both technical and non-technical).

91. Surrey Police is required to adhere to the PNC Code of Connection to maintain its access to the system. Under this code, Users of the Police National Computer are required to attend training before they may become authorised users. This training is provided by the Force Learning and Development Team, IT Faculty in accordance with nationally agreed standards.

92. Individual use of PNC is monitored and can be audited. While logged in, a user's username is used to generate an audit trail for every auditable action performed.

93. Users also receive training with regard to the Data Protection Act so they are aware of their obligations in relation to the handling of personal data. All staff sign the Official Secrets Act.

94. As previously disclosed in paragraph 57, personal browsing or use of applications or the information contained in them is not permitted under any circumstances.

95. PSD investigates all reported incidents of misuse of PNC. Normally these would be investigated as potential Gross Misconduct (that is misconduct that could, if proved, result in dismissal) rather than Misconduct. All staff joining the force are given the 'Surrey Police Security Matters' handbook (Exhibit **JK/5**) where it clearly states that inappropriate use of its systems will not be tolerated and that all breaches will be investigated. It also refers the reader of the need to comply with the use of Surrey Police computer systems policies.

17. What training is provided to individual users of the PNC to ensure that they understand what is and what is not lawful/appropriate use of the information held on the PNC?

96. All those permitted to use PNC are trained by National Police Improvement Agency (NPIA) approved trainers and complete courses dependant on the level of access and functions they need to perform. The basic course is five days. All courses include instruction on what is lawful and appropriate.

(18) What systems and/or measures are in place to audit the use of the PNC by Surrey police personnel? Describe the system of auditing, if any, that is in place.

97. All authorised operators and administrators of PNC are instructed they will abide by Surrey Police PNC Policies and Procedures and the NPIA PNC Manual.

98. Should PSD need to make enquiries into the appropriate use of a PNC operator they are able to make historic checks of all transactions.

(19) Do you consider that the systems and/or measures referred to in question (18) above work effectively? What changes, if any, do you consider should be made to them?

99. I believe that the system works reasonably effectively and can be demonstaretd by our low number of unlawful disclosures of PNC information, however we are not, and can never be, complacent. The fact that audit checks are randomly generated if required acts as a deterrent and increases the chances of detection of misuse rather than acting purely on intelligence of impropriety which is also possible when required.

(20) In the last 5 years:

a. How many suspected unlawful disclosures have there been of information held on the PNC by Surrey police personnel to the media and/or private detectives?

b. How many investigations have there been into those suspected unlawful disclosures of information? What was the outcome of those investigations?

100. Between 14/03/07 and 13/03/12 there have not been any identified incidents of unlawful disclosure of information held on PNC to the media or private detectives and, accordingly, there have not been any investigations into such disclosures.

(21) Do you consider that the unlawful disclosure of information from the PNC by Surrey Police personnel is a current problem? Please explain your answer.

101. Surrey Police have investigated 12 allegations of unlawful disclosure of PNC information by police personnel over the last 5 years. As already highlighted in paragraph 88, a number of these cases have related to casual interest rather than corrupt practices. These relatively low numbers of disclosures in company with the circumstances behind them do not give me significant concern or rise to believe that Surrey Police have security access problems. However, I do not remain complacent and ensure that any system security breaches or allegations of unlawful information disclosure rare investigated and any procedural or technological weaknesses are identified and resolved.

(22) Were changes made to any policies, procedures or systems relating to use of the databases and the security of the same following Operations Motorman, Glade and Reproof? If so, please specify.

102. I am not aware of any changes made after these operations. However Surrey Police policies and procedures are based on national guidance, so any changes implemented on a national basis as a result of these operations would be captured within our own.

(23) What additional measures, if any, should be put in place to prevent the unlawful disclosure of information held on the PNC and Surrey police's own databases? The documents you should provide to the Inquiry Panel are:

(a) Documents recording the systems and measures referred to above (limited to the last 5 years);

(b) Instructions/guidelines for users of the databases (limited to the last 5 years).

103. Surrey Police has articulated its local Information Risk Appetite as 'Open'. This means that the force is willing to consider all options and choose the one that is most likely to result in successful delivery while also providing an acceptable level of business benefit. This risk appetite has been partly driven by fiscal pressures and also by the desire to make users more flexible and mobile through the use of technology.

104. The Information Risk Appetite for National Systems such as PNC is 'Cautious'.

105. The systems and measures outlined in the answers above are effective to a point. As a police force, we obtain and are entrusted with a large amount of personal information. Much of that information needs to be accessed relatively easily by a large number of staff so that they can prevent and detect crime efficiently. We have to balance that need with

the need to protect personal information from unnecessary or unlawful access or disclosure.

106. By its very nature, the information held on our databases is of interest to people outside the force who may come into contact with one of Surrey Police's 4,174 staff and attempt to obtain that information. Surrey Police attempts to prevent this happening by having adequate security arrangements, clear acceptable usage polices and responding robustly when inappropriate or unlawful use of the databases is identified.

107. The vast majority of application users behave appropriately and ensure that the information entrusted to us is protected. However, despite the measures the force has put in place, Surrey Police still occasionally has deal with individuals who choose, for a variety of reasons (ranging from corruption to casual interest), to step outside of force policy, or in the case of PNC, national guidelines. I suspect that this would be the case regardless of the policies, training and security measures that police forces put in place if an officer is sufficiently determined to misuse personal information. Such an officer knows that he or she would face disciplinary (and, where appropriate, criminal) sanction if they were caught which for the vast majority of officers provides a sufficient deterrent. Surrey Police remain committed to information security and are always intent on identifying and incorporating new procedures and practices that will strengthen our system defences.

I believe the facts stated in this witness statement are true

Signed.[redacted].....

Dated......21 · 3 · 12......