



GLOBAL OPERATING PROCEDURE for DATA PROTECTION

This Procedure applies to all BBC's Divisions, including the BBC Trust.

In addition to this 'Global' Procedure, each Division has its own specific procedure which captures the local arrangements in place to deliver compliance with the Data Protection Act and associated legislation (the Act), the BBC's Data Protection Handbook (DP Handbook) and any instructions provided by Information Security (IS). This regime exists to ensure personal data held by the BBC is properly protected and to provide BBC management with systems assurance.

The Information Policy and Compliance department (IPC) is available to offer advice on how to interpret and work in compliance with the Act and the DP Handbook. The IS team is available to offer advice on the technical measures required in order to protect personal data.

Who to contact for advice:

Please see this link for the up-to date Data Protection Representatives and Contacts [\[add link\]](#)

Contents:

1. Data Protection Activities
2. Advice and Approval
3. Legal and Contractual Responsibility
4. Reporting Data Protection Compliance (See Half-Yearly Return Template and Guidance)
5. Training
6. Data Protection Audits
7. Risk Reporting
8. Subject Access Requests and other Data Subject Rights
9. Data Security Breaches
10. Outsource Service Providers
11. Approaches from the ICO
12. Review and Updates to Procedure

1. Data Protection Activities

Each Division in the BBC processes personal data. However, the circumstances in which personal data is processed varies greatly, both inside individual groups as well as between divisions. Each Division shall maintain a Register of Data Protection Activities that provides an overview of all activities in the Division in which personal data are processed.

This Register shall be reviewed and approved by the Division and IPC on a 6 monthly basis.

2. Advice and Approval Processes

BBC

The advice and approval of IPC (and IS where appropriate) must be sought if there is any question or uncertainty regarding compliance with the Act or the DP Handbook. You should contact your IPC Adviser or information security who will advise and provide necessary approval and highlight any other consultation that might be necessary. IPC retains a log of advice provided by the IPC team, to maintain precedent, consistency and to demonstrate compliance.

3. Legal and Contractual Responsibility

Every person working at the BBC (employees, contractors and freelancers etc) must only deal with personal data in accordance with the Act, the DP Handbook and the Computer Misuse Act, and also appropriate guidance from the Information Commissioner (eg Employment Practices Code).

Data Protection is so important at the BBC that if employees breach this policy it may result in disciplinary measures being brought against them.

This is linked with your rights and responsibilities set out in the Acceptable Use Policy

Everyone is responsible for ensuring that personal data is kept secure in accordance with any applicable guidance issued by BBC Information Security ism@bbc.co.uk.

The Divisional Procedures outline who in each division will fulfil the particular roles of the DP Representative, DP Contacts and IPC advisers.

4. Reporting Data Protection Compliance

4.1 At the end of the 2nd and 4th quarter (at 30 September and 31 March), each Division is required to report on compliance with the DP Handbook and Procedures.

Standard form reports known as Returns provide:

- Representation from the Division's Director that the Division has maintained awareness of DP issues throughout the preceding quarters;
- Summary of significant changes to the DP Activities Register;
- Update on any Data Protection issues or security breaches arising from previous half yearly meeting;
- Detail on any progress made with Data Protection audit or risk issues; and
- Training statistics

The DP Return is prepared by the designated DP Representative and signed by the Divisional Director.

BBC

The DP Return must be submitted to the IPC department by 31 October and 30 April respectively.

The DP Representative will meet with the relevant IPC Advisers in November and May to discuss each Return, the Register of Data Protection Activities, progress on audit issues, training, security issues, major issues and any other matters arising. The IPC Adviser will record any action points and report progress against them in the next Return.

- 4.2 From time to time it may be necessary to instigate a period of additional or more detailed reporting by specific business units, because there is heightened Data Protection risk or systems risk in that area. In these cases the Head of IPC or IPC Adviser will contact the Divisional Director and/or the DP Representative to agree the reporting requirements.

5. Training

Data protection training must be undertaken at least once every 3 years and is applicable to BBC staff as set out below.

Face to Face Training

The DP Representative will identify the people within the Division who require Face to Face DP Training. This list will be reviewed at the May meeting with the IPC Adviser.

As a minimum the list for Face to Face training will include (unless otherwise agreed with IPC):

- DP Representative
- DP Contacts
- Legal and Business Affairs staff
- All finance and HR staff
- All IT Co-ordinators

- other classes of staff that are identified in the Division Procedures. Individuals identified as requiring Face to Face training will be exempt if on maternity or other long-term leave.

The DP Representative will be required to report on the number of people who have completed the training as at the last day of the reporting period (31 March and 30 September). On that date **at least 95%** of staff identified as requiring Face to Face Training must have completed the training¹.

¹ For the purposes of reporting period ending 31 March 2009 only, Face to Face training compliance figures may include those who have completed the Online Training module



Online Training

Data protection online training is compulsory for all staff and freelancers with a BBC login except for individuals:

- Working outside the European Economic Area (except those in Switzerland, Guernsey; Isle of Man and Jersey)
- Who have received face to face data protection training;
- on maternity or other long-term leave;
- specifically been exempted by IPC from undertaking the training

The DP Representative will be required to report annually on the number of people who have completed the training as at 31st March. On that day **at least 80%** of staff identified as requiring Online Training must have completed the training.

6. Data Protection Auditing

BBC's Data Protection compliance regime will be subject to rolling audits undertaken by both internal and, on occasion, external auditors, as advised from time to time.

7. Risk Reporting

Data Protection Compliance will be reported Half Yearly Compliance Report as well as the General Counsel's Annual Legal Risk report.

8. Subject Access Requests and Requests to Stop Processing Personal Data

All individuals have certain rights under the Act in relation to the way the BBC handles their data. Where Divisions receive a Subject Access Request or a Section 10 Request they will forward them immediately to IPC.

Subject Access Requests

Any individual may request, in writing and on payment of £10 to the BBC, a copy of all the data the BBC holds about them. This is subject to a number of exemptions. Please forward all subject access requests to IPC.

All Data Protection subject access requests and requests under received by BBC must be handled promptly in accordance with the published guidance. These requests must be complied with in 40 calendar days.

B B C

The IPC team will co-ordinate the response to the requester; the DP Representative and their selected DP Contacts will have the responsibility for collecting all the relevant information from within the Division where IPC require their assistance.

“Section 10 Requests” Processing Causing Unwarranted Damage or Distress

Individuals may, pursuant to s10 of the Act, request that the BBC cease, or not being processing their data if it would cause *substantial damage* or *substantial distress* and that damage or distress is *unwarranted*. These requests must be in writing and the individual must establish why this unwarranted damage or distress would occur.

There are a number of exemptions to the application of section 10 (eg in relation to the BBC’s journalistic output) so it is imperative that all s10 requests are forwarded to IPC.

“Section 11 Requests” Direct Marketing

Where the BBC sends Direct Marketing (eg programme newsletters) it must always provide an accessible means for individuals to request that BBC stops this direct marketing activity (eg “Unsubscribe” button). See the DP Handbook for further information or contact IPC with questions. DP Representatives must ensure that where marketing activities are conducted in their Division that they comply with these requirements.

9. Data Security Breach Procedures

Where a data security breach² occurs the DP Representative or IPC must be immediately informed and the Data Security Breach Procedures must be followed.

10. Outsource Service Providers (OSP)

The DP Representative or the DP Contact will liaise with the IPC Adviser and the OSP regarding the Data Protection compliance of the OSPs working for the Division who also process large amounts of personal data on behalf of the BBC.

The DP Representative or relevant DP Contact will attend quarterly OSP Security and Data Protection Meetings (where they exist) and act on any actions identified in those meetings.

11. Approaches from the Information Commissioner’s Office (ICO)

² Data Security breach is: Loss/disclosure/inappropriate access or mishandling of either:

- Large volumes of personal data (ie details of more than 100 individuals)
- Personal data that that could cause potential harm to the individuals (eg financial/credit card details for a small number of staff); or
- Particularly sensitive data for smaller volumes (eg medical records, contract details of key talent, contact details of anonymous sources)

B B C

If a Division is contacted by the ICO they should immediately contact their IPC Adviser who will co-ordinate the response to the ICO.

12. Review and Updates to these Procedures

These Procedures (and the Divisional Procedures) are reviewed at least annually and are updated as required, in order to ensure that they continue to reflect best practice. In particular the following issues are considered:

- whether levels of awareness of the Act and the DP Handbook are being maintained; and
- whether the reporting framework and referral levels are ensuring that Data Protection issues are being captured.

B B C