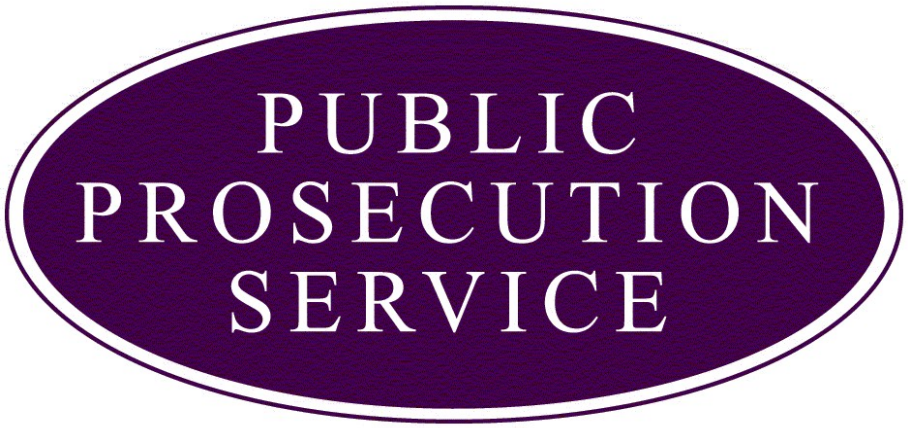

DATA PROTECTION POLICY STATEMENT

Version History

Number of this Version: 2.3

Date of this Version: 10 March 2011

Status: Final

Approved by SMG: 6 June 2011

Introduction

1. The Public Prosecution Service (PPS) is committed to complying fully with the Data Protection Act 1998 (the DPA) which came into force on 1 March 2000 and the Freedom of Information Act (FOIA) which came into force on 1 January 2005.

2. We will ensure that all employees, our Criminal Justice partners, contractors, agents, consultants and anyone else who has access to any personal information held by, or on behalf, of PPS is fully aware of and abides by their duties and responsibilities under these Acts.

Statement of Policy

3. PPS needs to collect and use information about people it deals with so that we can carry out our business. These include, but are not limited to:

   - Members of the public (e.g. victims, witnesses and defendants);
   - Current, past and prospective employees;
   - Clients, customers and suppliers.

4. We will handle and deal with properly all personal information however it is collected, recorded or used.

Data Protection Principles

5. PPS fully supports and will comply with the eight principles of the DPA. This means that personal information must be:

   1. Processed fairly and lawfully;
   2. Processed for limited purposes and in an appropriate way;
   3. Relevant and sufficient for the purpose;
   4. Accurate;
   5. Kept for as long as is necessary and no longer;
   6. Processed in line with individual's rights;
   7. Secure;
   8. Only transferred to other countries that have suitable data protection controls.

6. The majority of the data processed by the PPS relates to the prosecution of offenders. Section 29, 1(b) of the DPA provides that data processed for the purpose "of the apprehension or prosecution of offenders" is exempt from principle 1 of the Data Protection Act (except for the requirement that the processing must satisfy one of the conditions in schedule 2). Nevertheless the PPS will comply with the requirements of Principle 1 as far as possible.

7. All data processed in the PPS must meet one of the conditions in Schedule 2. In the case of the PPS these are:

- paragraph 5(a) – “for the administration of justice.”
- paragraph 5(c) – “for the exercise of any functions of the Crown, a Minister of the Crown or a government department”

8. The PPS is also exempt from the requirements of Principle 8 in respect of data transferred “for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),” (Schedule 4, paragraph 5(a))

Notification of Data Commissioner

9. The PPS has notified the Information Commissioner’s Office that it acts as a Data Controller under the DPA. Our purpose for holding personal information and a general description of the categories of people and organisations to which we may disclose it are listed in the Information Commissioner’s Data Protection Register (http://www.ico.gov.uk/ESDWebPages/Search.asp).

Handling of Personal Information

10. We will give all our staff appropriate training and manage them so that PPS can be confident that it is:

- Fully observing conditions regarding the fair collection and use of personal information;
- Meeting our legal obligations to specify the purposes for which personal information is used;
- Collecting and processing appropriate personal information only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
- Ensuring the quality of personal information used;
- Applying strict checks to determine the length of time personal information is held;
- Ensuring that the rights of people about whom information is held can be fully exercised under the Act;
- Taking appropriate technical and organisational security measures to safeguard personal information;
- Ensuring that personal information is not transferred abroad without adequate safeguards.

Compliance

11. PPS will ensure that:

- We have a clearly identified focal point with specific responsibility for Data Protection in the organisation;

- We make all staff aware of the DPA and FOIA on appointment and at least annually;
- Everyone managing and handling personal information understands that they have a direct and personal responsibility for following best Data Protection practice;
- We only give access to personal information to staff who need it as part of their duties;
- We appropriately supervise everyone managing and handling personal information;
- We deal promptly and courteously with queries about the handling of personal information;
- Any member of PPS staff who has a query about handling personal information knows who to ask or where to look for advice;
- We clearly describe and make accessible the way in which personal information in PPS is to be handled;
- We regularly assess and manage the risks to personal information;
- We formally audit the way in which personal information is handled;
- We properly report and investigate losses or compromise of personal information.

Corporate Responsibilities

12. To support compliance and to ensure that work on Data Protection is fully integrated with work on other Information Assurance activities, PPS has created the new roles of:

- Senior Information Risk Owner – the Acting Senior Assistant Director, Corporate Services;
- Information Risk & Asset Owners – Assistant Directors / Regional Prosecutors and Heads of Branch in Corporate Services;
- Business Assurance Manager – based in Corporate Services.

Details of the roles and responsibilities of each of these are set out at Annexe “A”.

Individual Responsibilities

13. Every member of staff has a personal responsibility to protect the personal information held by PPS and must keep personal information secure at all times against unauthorised or unlawful loss or disclosure. Individual members of PPS staff must:

- Ensure that they have received training in the handling of personal information;
- Keep all personal information, whether held in electronic or paper format, in a secure environment;
- Ensure that passwords that give them access to personal information are protected and are not disclosed or shared;

- Comply with any published guidance and procedures;
- NOT disclose personal information held on others for unauthorised purposes.

Disclosure of Personal Information to Third Parties

14. The PPS discloses personal data to third parties for the purpose of "of the apprehension or prosecution of offenders". This disclosure is exempt from principle 1 of the Act. We do not require the subject's consent to disclose data for this purpose.

15. Where we disclose personal data to third parties for any other purpose, we must comply with all the data protection principles. We only exchange information when we believe that it is lawful to do so and:

    - The subject has consented to the disclosure, or;
    - The information is in a form that does not identify the subject.

16. In all circumstances, we will ensure that the necessary steps are taken to protect such information during its transportation and processing.

17. Any third parties who are supplied with personal information by PPS in any format will be required to confirm and demonstrate that they are abiding by the requirements of the Act. They may be required to enter into an Information Sharing Agreement with PPS to regulate the sharing and use of such data. Audits may be carried out by PPS to confirm compliance.

18. Any member of staff who has a doubt or concern about the sharing of personal information with a third party must seek immediate advice from the PPS Business Assurance Manager.

Awareness

19. A copy of this policy statement will be given to all new members of staff on induction. Existing staff and third parties will be advised of the policy via the PPS Intranet and Internet sites. Revisions will also be publicised via these sites.

Annex A

DATA PROTECTION, DATA HANDLING AND INFORMATION ASSURANCE – ROLES AND RESPONSIBILITIES

The Senior Information Risk Owner (IRO)

The Senior Information Risk Owner in PPS is the Assistant Director, Corporate Services. He will:

- Lead and foster across PPS a culture that values, protects and uses information for the public good;
- Own the PPS Data Protection policy, its information risk policy and the risk assessment process, ensuring that the latter is used effectively;
- Advise the Director on all aspects of DPA and FOIA compliance and on the information risks (and the steps being taken to mitigate them) in PPS.

Information Risk & Asset Owners (IAO)

Each Assistant Director / Regional Prosecutor in PPS and each Head of Branch in Corporate Services is an Information Asset Owner. They will:

- Lead and foster a culture in their own business area that values, protects and uses information for the public good;
- Knows what data and information is held in their business area, how it is used and shared, and why;
- Knows who uses that data in their business area and why and ensures that its use is properly monitored;
- Understands and mitigates any risks to information and data in their business areas and provides assurance on management of risk to the IRO;
- Ensure that there are effective arrangements for responding to requests for access from others.

Business Assurance Manager

The Business Assurance Manager is a Head of Branch in PPS Corporate Services. He will:

- Provide professional expertise in the DPA, the FOIA and Government data handling requirements;
- Act as DPA Compliance Officer;
- Develop Information Risk policy and identify and manage emerging risks;
- Map the key information and data assets held by PPS;
- Identify and make recommendations about improvements to the handling and security of information and data in PPS;
- Act as a focal point for advice to PPS staff on all aspects of data protection and information risk;
- Conduct awareness training and briefings.