

PRESCRIPTION PRICING AUTHORITY

DATA PROTECTION

1. POLICY STATEMENT

- 1.1 This document defines the Data Protection Policy for the PPA.
- 1.2 The Data Protection Policy applies to all personal information obtained and processed by the PPA and the Authority's employees.
- 1.3 This document:
 - Sets out the organisation's policy for the protection of all information obtained and processed.
 - Establishes the responsibilities for Data Protection.
 - Provides reference to the Data Protection Act 1998.

2. PRINCIPLES

- 2.1 The objective of this policy is to ensure the protection of PPA's information in accordance with the Data Protection Act 1998, that is:
 - To ensure notification;
Annually notify the Information Commissioner about the purposes of PPA's systems that process personal information.
 - To ensure professionalism;
All information is obtained, held and processed in a professional manner in accordance with the eight principles of the Data Protection Act.
 - To preserve security;
All information is obtained, held and disclosed in a secure manner.
 - To ensure awareness;
Proper training and awareness is in place which informs all employees of their roles and responsibilities.
 - Data Subject access;
Prompt and helpful response to any data subject access request.
- 2.2 The policy and procedure will be reviewed periodically by the Human Resources Department. Where review is necessary due to legislative change this will happen immediately.

- 2.3 In accordance with the Authority's Equal Opportunities policy, this procedure will not discriminate, either directly or indirectly, on the grounds of gender, race, colour, ethnic or national origin, sexual orientation, marital status, religious beliefs, age, union membership, disability, offending background or any other personal characteristic.

3. SCOPE OF THIS POLICY

- 3.1 This policy applies to all personal information processed, stored on computer or structured filing systems (manual records), or Close Circuit Television and any extracts taken either printed, copied, or verbal and the Authority staff who use the information in connection with their work.

4. POLICY

- 4.1 The overall Data Protection Policy for the PPA is described below:

- 4.2 The PPA needs to obtain and process information about different people for many purposes for example database of health practitioners, pharmacists, prescription processing, low income benefits, staff records and administrative records. Such information may be kept in either computer or manual records. In processing such personal data PPA will comply with the data protection principles within the Data Protection Act 1998. The principles are:-

- Personal data shall be processed fairly and lawfully. Individuals will be advised why the PPA is collecting their information, why it is held, used and to whom it may be shared.
- Personal data shall be obtained only for one or more specified and lawful purpose as outlined in the notification to the Information Commissioner. Information is collected for a specific use and no other. Further use will only be undertaken with the consent of the individual, or by law.
- Personal data shall be adequate, relevant and not excessive. Information collected will be the minimum required to complete the necessary PPA business function.
- Personal data shall be accurate and kept up to date. The PPA will take necessary steps to ensure accuracy of information through sample monitoring where appropriate.
- Personal data shall not be kept longer than necessary. Records where appropriate will be reviewed and weeded in accordance to PPA policy.
- Personal data shall be processed in accordance with the rights of the individual. PPA complies with the rights of an individual to access their records and be provided with a copy. The PPA enables individuals to exercise their right to request the prevention of processing of their information which is likely to cause damage and distress, a prompt response will be issued. The PPA does not

use individual information for direct marketing purposes, or for automated decision making.

- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss, destruction, or damage. BS 7799 requirements are complied with to ensure security of PPA systems.
- Personal data shall not be transferred to a country/territory outside the EEC unless the appropriate security and protection of personal data can be guaranteed. The PPA does not transfer information outside of the EEC.

Where relevant the PPA will comply with:

- Regulation of Investigatory Powers Act 2000
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Obscene Publications Act 1959
- Telecommunications Act 1984
- Protection of Children Act 1978
- Criminal Justice Act 1988
- Copyright, Design and Patents Act 1998
- Protection from Harassment Act 1997
- Sex Discrimination Act 1975
- Race Relations Act 1976
- Computer Misuse Act 1990
- Common Law, that is, ensure that normal civil responsibilities apply. Information will only be used for the purpose for which it was intended.

5. DATA PROTECTION RESPONSIBILITIES

Overall Responsibilities

- 5.1 The Chief Executive, as Data Controller permits PPA staff to use computers and relevant filing systems (manual records) only in connection with their work. He has legal responsibility for the notification process and compliance of the Data Protection Act 1998.
- 5.2 The Chief Executive, whilst retaining his legal responsibilities has designated Data Protection compliance to the Data Protection Officer, Director of IT.

Data Protection Officer's Responsibilities

- 5.3 The Data Protection Officer responsibilities include:
 - Ensuring that appropriate Data Protection Act policy for the Authority is produced and kept up to date.
 - Ensuring that the appropriate procedures and practices are formulated and adopted by the PPA.
 - Representing the PPA on Data Protection matters
 - Providing the appropriate leadership and direction for the Data

Protection team operating within the PPA.

Data Protection Officer's Responsibilities (as delegated)

- 5.4 The Data Protection Officer has delegated the daily responsibilities to the Data Protection Manager who is assisted by the Data Protection Teamleader. Their responsibilities are:
- Ensuring the Data Protection notifications are reviewed, maintained and renewed annually for all applicable systems.
 - Ensuring compliance with individuals rights, including subject access.
 - Assisting in the preparation of policies, procedures, protocols and guidance in compliance with Data Protection.
 - Ensure staff training and awareness of their responsibilities in Data Protection.
 - Providing advice and guidance to all enquiries from internal and external sources.
 - Monitor compliance with the Data Protection Act, any infringement i.e. unlawful disclosure of information or access for idle curiosity are investigated and appropriately dealt with.
 - Audit appropriate systems in accordance with risk analysis reviews.
 - Acting as a central point of contact on data protection within the organisation.
 - Implementing an effective framework for the management of data protection.

Line Manager's Responsibilities

- 5.5 Line Managers are directly responsible for:
- Ensuring that their staff are made aware of any Data Protection notices.
 - Ensuring that their staff are aware of their Data Protection Responsibilities.
 - Ensuring that their staff have had suitable Data Protection training.

General Responsibilities

- 5.6 All PPA employees are subject to Data Protection compliance and this policy, they are accountable via personal liability.

6. VALIDITY OF THIS POLICY

- 6.1 **THIS POLICY IS DESIGNED TO AVOID DISCRIMINATION AND IN ACCORDANCE WITH THE HUMAN RIGHTS ACT 1998 AND ITS UNDERLYING PRINCIPLES.**
- 6.2 This policy should be reviewed annually under the authority of the Chief Executive. Associated Data Protection standards should be subject to an ongoing development and review programme.