

INFORMATION SECURITY

POLICY STATEMENT

OBJECTIVE

The objective of this document is to state the PPA's approach to meeting its statutory obligations to ensure the confidentiality of, and prevent any unauthorised access to, or use of, all information received or generated within the PPA.

INTRODUCTION

Information security management enables information to be shared, at the appropriate level, while ensuring the protection of information and computing assets. Its basic components are:

- a) Confidentiality, - protecting sensitive information, including intellectual copyright, from unauthorised disclosure or intelligible interception;
- b) Integrity, - safeguarding the accuracy and completeness of information and computer software;
- c) Business continuity, - plans for the speedy restoration of critical business processes in the event of business interruptions;
- d) Incident prevention, - preventing and minimising the impact of deliberate or accidental acts which result in breaches of confidentiality, corruption, and/or loss of vital information or vital services;
- e) Availability, - ensuring that information and vital services are available to users when required;

Information takes many forms and many methods can be used to convey knowledge and ideas. It can be stored on computers, transmitted across networks, printed out or written down on paper, and spoken in conversations or over the telephone. The appropriate protection should be in place to cover all these aspects.

POLICY

The Authority's information security policy is to preserve the confidentiality, integrity and availability of the organisation's systems and data. It is essential that all information processing systems and data are protected to an adequate level from events which might jeopardise performance of the PPA's business objectives. These events will include accidents as well as behaviour deliberately designed to cause difficulties.

This policy covers all verbal, written, printed or stored information, whether in a paper or electronic form.

This policy embraces the requirements of the Data Protection Act (1998), the Computer Misuse Act (1990), the Copyright, Designs and Patents Act (1988), The Common Law

Duty of Confidentiality, the Access to Health Records Act (1990), the Access to Medical Records Act (1988) the Personal Files Act (1987).

The most relevant guidance for Information Security is published as a British Standard, BS7799, and as NHS Guidance, IM&T Security Manual IMG Ref. E5501.

POLICY DELIVERY

The policy of the Authority shall be delivered by ensuring the use of best practice enshrined within appropriate, published, standards and procedures:

- Appropriate protective measures to be applied shall include control of visitors and restriction of physical access to PPA premises and areas housing PPA information assets to authorised persons.
- Access to PPA systems and data by outside third parties to be limited, restricted and controlled by an appropriate signed agreement and hardware and software mechanisms and in conformance with the PPA's Data Protection Act obligations.
- Information to be protected against unauthorised access by the use of unique identifiers, passwords and logical access software, segregation of duties and where necessary, encryption.
- Confidentiality of information to be assured by prevention of unauthorised access or disclosure, a policy for formally recording release of information to external, third parties, and where necessary, encryption.
- Integrity of information to be maintained by virus controls, application and database designs, appropriate business processes and audit trails.
- Contracts of employment to contain the necessary clauses relating to the duty of confidentiality obliging an officer to respect and preserve the confidentiality of all information to which he has access, either as an employee of the Authority, or after leaving the employ of the PPA.
- Job descriptions to define specific security roles and responsibilities for implementing or maintaining security policy, protection of assets or for particular security processes or activities.
- Education to be given to officers for their specific information security roles and responsibilities.
- Ongoing publicity programme to remind officers of their information security obligations.
- Controls to be in place for the removal of equipment and/or magnetic media, such that removal is subject to an appropriate signed agreement and release to the named responsible person.
- Appropriate procedures and mechanisms to be in place to protect information assets entrusted to officers working off-site.
- Business continuity plans to be produced, tested and maintained.
- All PPA managers to be directly responsible for implementing this Policy within their business areas, and for adherence by their staff to the Policy and its associated standards and procedures.
- Appropriate conduct and disciplinary procedures to be in place to deal with any breach of security.

- The PPA's Data Protection registration to be maintained and renewed when required to ensure regulatory and legislative requirements are met.
- A formal Information Security Manual to be created for each division of the Authority, to contain those information security standards, processes and procedures pertinent to each particular division.
- Audit procedures to be in place to confirm compliance and effectiveness of the information security standards and procedures.
- Appropriate software tools to be used to protect and monitor security processes and to detect attempted breaches.
- All breaches of information security, actual or suspected, to be reported to, and investigated by the Information Security Manager.
- The Information Security Manager to monitor all breaches, determine their cause, report on the suitability of the policy for protection of the Authority's assets, and advise on best practice.

The Information Security Manager shall review this policy on an annual basis to ensure that its contents are current and still reflect best practice.

A formal annual report of the state of information security within the Authority shall be produced for the Chief Executive.

It is the responsibility of each employee to become familiar with the Authority's information security requirements, and to adhere to this policy.