ISPS-011

Working in partnership

Information Security Policy Suite

Data Protection Policy

This policy is available in alternative formats upon request, such as large print or electronically. Please contact the Information Security Manager, to obtain a copy in a different format.

Approval Authority: Cabinet Member for Finance and Service Delivery Approval Date: December 2012

Data Protection Policy

1. Purpose

The purpose of this policy is to ensure appropriate measures are applied to comply with the eight principles of the Data Protection Act 1998 ('the Act') and so to meet the Councils' statutory requirements under the Act.

2. Scope

This policy applies to all staff, members, contractors and any other persons who have access to the Council's information, information systems and networks.

This policy applies to all information held, created, modified or accessed from the effective date of this policy. It includes information in any form, no matter whether it is stationary (e.g. an electronic or paper document) or in transit (e.g. file transfer, e-mail, fax, phone, post, courier). It also covers the buildings, premises and systems which contain that information refer to the Buildings, Infrastructure and Equipment Security Policy (ISPS-004).

3. Policy Statement

The policy of the Council is to ensure that it takes appropriate technical and organisational security measures that require that personal information is:

a. Processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met;

b. Obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes;

c. Adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed;

d. Accurate and where necessary, kept up to date;

e. Not be kept for longer than is necessary for that purpose or those purposes;

f. Processed in accordance with the rights of data subjects under this Act;

g. Protected against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data;

h. Not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

3.1 Data Subject Access Requests (SAR)

a. All Subject Access Requests for information made to the Council under the Data Protection Act 1998 will be dealt with by the designated officers, and in accordance with the Council's Data Protection Code of Practice.

b. Access will be afforded in accordance with the Act to data subjects applying for such information in the specified manner, for which a fee of £10 will be charged. No fee, however, will be charged to employees or Members for information relating to their employment or duties.

4. Responsibilities

This section should be read in conjunction with the responsibilities detailed in section 4 of the Information Governance and Security Policy (ISPS-001). Additional responsibilities arising from this policy are specified below.

4.1 Data Protection Officer

Their responsibilities include:

a. The maintenance of the Council's compliance;

b. Annual renewal of notification registration;

c. Dissemination of data protection information within the authority;

d. Dealing with changes and modifications arising from legislation or codes of practice.

4.2 Managers

It is the responsibility of Managers to ensure compliance with this policy within their own service areas. Their responsibility includes:

a. Ensuring that staff are aware of their responsibilities under the Data Protection Act

b. Ensuring employees, including contractors, consultants and volunteers employed to undertake Council business follow the data protection policy and procedures

c. Ensure appropriate resources are in place to enable compliance with the data protection policy

In addition, it is the responsibility of Heads of Service to ensure that any new computerised or manual systems are compliant with the Data Protection Act and that they notify the designated officer of any known future developments likely to affect the Council's notification.

4.3 Staff

a. All staff must be aware of the Data Protection Act, and of their obligations under it.

b. Individual staff members may be personally liable for breaches of the Act if they act outside the authority of the data controller.

c. All new members of staff must sign a non-disclosure document and will receive information about the Council's Data Protection Policy and procedures as part of their induction process and in training sessions provided by the Council.

d. Refresher training will be carried out for all staff on a regular basis, in particular when there are any changes in legislation, when there is an information security incident or on a three yearly cycle at the Council's discretion.

4.4 Members

a. All elected Members should be made fully aware of this policy and of their duties and responsibilities under the Act.

b. When Members handle personal information in their role as politicians or in their role as elected members, they are covered by their party or the Council's notification respectively. As such, they have to handle personal information in line with the requirements of the Council's Data Protection Policy.

c. If Members use (process) personal information in their constituency work, or are independent elected Members, they must notify with the Information Commissioner's Office as a data controller in their own right.

5. Training associated with this Policy

This policy will be included in the Information Security suite of awareness materials and training courses and delivered with reference to the Training Guidelines (ISPS-001b1).

If anyone requires support, advice or guidance on any element outlined in this policy they should speak with their line manager.

6. Monitoring

Compliance monitoring will be carried out by the Council's Information Security Manager (ISM) and through the Council's management structure.

6.1 Non-compliance

Disciplinary action in accordance with procedures approved by the Council may be taken against any employee who breaches the requirements of this policy.

6.2 Review

This Data Protection Policy will initially be reviewed after twelve months and on a three-yearly basis thereafter, refer to the review procedure in Appendix A of the Policy Creation and Style Guidelines (ISPS-001b3).

7. Equality Impact Assessment (EIA)

An equality impact assessment has been completed for the whole Information Security Policy Suite. A copy of the form is available upon request from the Council's Information Security Manager (ISM).

8. Related documents

This policy should be read in conjunction with the following documents:

- ISPS-001 Information Governance and Security Policy;
- Other policies in the Information Security Policy Suite;
- Any supporting standards, guidelines and procedures.