****

**Scottish Law Commission Records Management Plan**

**Data Protection Policy Statement**

**Document control**

|  |  |
| --- | --- |
| **Name of document** | **Data Protection Policy Statement** |
| **Drafted by** | **Head of Records Management** |
| **Approved by** | **Chief Executive** |
| **Date of approval** | **26 January 2015** |
| **Version**  | **1.0** |
| **Review frequency** | **Annually** |
| **Next review date** | **February 2016** |

**Introduction**

1. This Policy Statement has been prepared in support of Element 9 of the Commission’s Records Management Plan for submission to the Keeper of the Records of Scotland under the Public Records (Scotland) Act 2011.

**Obligations under the Data Protection Act 1998**

2. The Data Protection Act 1998 provides for the regulation of the processing of information relating to individuals including the obtaining, holding, use or disclosure of such information. It concerns the security of personal information and the rights of individuals to access information held about them.

3. Under the 1998 Act an authority must only collect personal information which is needed to carry out its functions, must keep it secure and ensure that it continues to be relevant and up to date. An authority must only hold as much personal information as it needs for business purposes and must not retain it any longer than is necessary for those purposes. A person who is the subject of any information must be given access to it on request.

4. The Scottish Law Commission needs to collect, process and hold certain personal information about Commissioners, staff, consultants, consultees, and others in connection with carrying out its functions.

5. This Policy Statement sets out the Commission’s obligations under the 1998 Act. It indicates the Commission’s commitment to ensuring compliance with the Act. The policy applies to Commissioners and all members of staff and relates to records in all formats including paper, electronic, audio, visual, and photographic.

**Data Protection Principles**

6. Part 1 of Schedule 1 to the 1998 Act sets out 8 principles relating to personal data. The principles are that personal data:

(1) personal data must be processed fairly and must not be processed unless certain conditions are met;

(2) personal data must be obtained for specified and lawful purposes and must not be further processed in a manner which is incompatible with those purposes;

(3) personal data must be adequate, relevant and not excessive in relation to the purposes for which they are processed;

(4) personal data must be accurate and where necessary, kept up to date;

(5) personal data processed for any purposes must not be kept for longer than is necessary for those purposes;

(6) personal data must be processed in accordance with the rights of data subjects under the 1998 Act;

(7) appropriate technical and organisational measures must be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data;

(8) personal data must 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.

**Meaning of “personal data” and “sensitive personal data”**

7. Section 1(1) of the 1998 Act defines “personal data” as “data which relate to a living individual who can be identified-

(a) from those data, or

(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.”

8. Certain personal data relating to an individual (“the data subject”) is subject to stricter regulation under the 1998 Act. Section 2 of the 1998 Act defines the meaning of “sensitive personal data” as personal data consisting of information as to:

(a) the racial or ethnic origin of the data subject;

(b) his personal opinions;

(c) his religious beliefs or other beliefs of a similar nature;

(d) whether he is a member of a trade union;

(e) his physical or mental health or condition;

(f) his sexual life;

(g) the commission or alleged commission by him of any offence;

(h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.”

**Responsibility for compliance with the Data Protection Act 1998**

9. All Commissioners and staff are required to comply with the data protection principles.

10. The Chief Executive as data controller has primary responsibility for ensuring that the collection and processing of personal data by the Commission is done so as to comply with the 1998 Act. The Records Manager is responsible for providing information on responsibilities under the Act, for supporting staff in complying with their obligations under the Act and for ensuring that all staff have data protection training.

11. All staff must familiarise themselves with the data protection policy and supporting codes of practice. They must ensure that they adhere to the procedures relating to the collection and use of personal data. In particular staff are required to undertake the online data protection learning package provided on the Scottish Government Intranet on an annual basis. A requirement to undertake this training should be included in staff personal learning plans as part of the appraisal system.

**Data protection policy statement**

12. The Commission is committed to ensuring that personal information is collected fairly, is stored securely and is not disclosed to any person unlawfully, in accordance with the Data Protection Act 1998.

13. In particular the Commission is committed to-

(a) making data subjects aware when collecting personal data about them and outlining the way in which the information will be used;

(b) observing the conditions about the use and retention of personal data;

(c) processing and retaining personal information only for so long as necessary for to carry out its functions;

(d) retaining records for only so long as necessary for business purposes;

(e) ensuring that data subjects can exercise their rights under the Act in relation to information it holds;

(f) ensuring that personal data is held securely;

(g) ensuring all staff are given induction training on data protection policy.

These are achieved by-

(a) the Chief Executive and the Records Manager being identified as having operational responsibility for data protection matters within the Commission;

(b) ensuring that all staff are aware of their responsibilities in relation to data protection;

(c); ensuring that personal data are only kept for so long as it is needed and that data are destroyed in terms of the retention schedules (for example personal data on legal assistants and work experience students);

(d) monitoring arrangements for the collection, processing, and management of personal data.

**Compliance with related legislation**

14. Compliance with this Policy Statement will contribute to compliance with the Data Protection Act 1998 and with related legislation including the following:

Human Rights Act 1998

Freedom of Information (Scotland) Act 2002

Equality Act 2010

Public Records (Scotland) Act 2011.

**Monitoring and review**

15. The Commission’s policy on data protection will be monitored by the Records Manager and Chief Executive on a regular basis to ensure compliance with the 1998 Act.