Data Protection Policy and Handbook

Scottish Information Commissioner

Scottish Information Commissioner

Contents

Glossary and abbreviations

Term used	Explanation
The Commissioner	The Scottish Information Commissioner
DPA	The Data Protection Act 1998
DP	Data Protection
FAM	Finance and Administration Manager
HOOM	Head of Operational Management
SAR	Subject access request
SIC	The Scottish Information Commissioner, staff/ office of SIC depending on context
SMT	Senior Management Team

Cross-referenced INVU documents (for internal use)

INVU No	INVU name
INV45232	This document
INV45262	Information and Records Management Handbook

Introduction

1. The Data Protection Act 1998 (DPA) imposes obligations on the processing of personal data held by the Scottish Information Commissioner (SIC) (essentially, all aspects of its management and use) and has implications for every part of the organisation. This policy sets out how the SIC complies with the DPA.

2. This policy and the related procedures and guidance aim to ensure SIC fulfils the requirement for fair and lawful processing of personal data in the records created and received in the course of its activities.

3. This policy complies with the DPA.

Policy Statement

4. SIC is a data controller, as defined in section 1(1) of the DPA, and is obliged to ensure that all of the DPA requirements are implemented. To do this, SIC complies with the eight data protection principles which are set out in the DPA (see Appendix I).

5. As part of normal business operations, SIC collects, holds and retains personal data about its employees and stakeholders . Where required, SIC gives those whose personal data is held (known as "data subjects") fair notice of the purposes for which their personal data is processed.

6. SIC ensures that personal data is collected and used fairly, is stored safely, and is managed in accordance with the data protection principles by ensuring that personal data is kept secure, accurate and up to date, and disposed of securely at the appropriate time.

7. SIC will not disclose personal data to any third party unlawfully.

Data subject to the Data Protection Act 1998

8. The DPA relates to the processing of personal data. Personal data is information that both identifies and relates to a living individual, and includes any expression of opinion about the individual. As a public authority, the DPA applies to all personal data held by SIC, both electronically and manually.

9. The DPA categorises some types of personal data as sensitive personal data. This includes personal data concerning racial or ethnic origin, political or religious beliefs, trade union membership, physical or mental health, sexual orientation and criminal records.

10. Particular care must be taken when sensitive personal data is being sent by post. Two people must check the envelope to confirm that the correct information is being sent to the recipient.

11. The majority of the personal data held by SIC is not sensitive and is made up of data provided by employees and stakeholders.

Right of access to personal data

12. An individual's right to request their own personal data is known as a subject access request (SAR).

13. SARs are requests to SIC for personal data made by the data subject (i.e. the person whose personal data it is). In some cases, a SAR may be made by a third party on that person's behalf, e.g. by

    - a parent on behalf of a young child
    - a representative on behalf of an adult with incapacity
    - a solicitor on behalf of a client.

14. SIC takes reasonable steps to make sure that the person making the SAR is who they say they are. If someone is making a request on behalf of a third party, SIC checks that they have the authority to make that request.

15. SIC's Enquiries Procedures provide full guidance to staff on how to respond to SARs.

Data Processors

16. Where SIC uses a contractor to process personal data on its behalf (a "data processor"), SIC must be satisfied that the contractor is taking adequate steps to allow SIC to meet its obligations under the DPA. Contracts between SIC and data processors must ensure that all necessary security procedures and other appropriate measures are specified in the contract, and the contract must be monitored to ensure that they are being adhered to.

Governance Arrangements

17. In order to comply with the DPA, in addition to this Policy, SIC has business processes and systems which include:

    (i) identifying a role with specific responsibility for Data Protection

    (ii) the provision and implementation of procedures for SIC staff on handling personal data.

    (iii) training for all SIC staff in data protection and good practice.

    (iv) the maintenance and application of retention and disposal schedules for all SIC records to ensure information is only retained for as long as it is required.

    (v) adherence to established information security procedures for both manual and electronic records, subject to appropriate risk assessment.

    (vi) notification with the Information Commissioner of all uses of personal data within SIC.

    (vii) an annual report on Information and Records Management to the Senior Management Team

Breaches and near-misses

18. In the event that a security breach (or a near-miss) does occur, it **must be reported immediately** to the FAM (in whose absence, the HOOM, which failing another member of the SMT).

19. The Information and Records Management Handbook (INV45262) sets out in full the arrangements for responding to data breaches and near misses.

Staff responsibilities

20. **All staff** are required to be aware of the provisions of the DPA and its impact on the work SIC undertakes.

Senior Management Team (SMT)

21. The SMT has overall responsibility for the Data Protection Policy.

22. The SMT is responsible for ensuring the policy and procedures for handling personal data are followed, and that staff competence is maintained and developed.

23. The Head of Operational Management has direct responsibility for overseeing the work of the Finance and Administration Manager.

Finance and Administration Manager (FAM)

24. The FAM has responsibility for ensuring that SIC's Data Protection Notification is kept up to date.

25. The FAM, in conjunction with the SMT, reviews and updates DPA procedures as necessary.

26. The FAM monitors compliance with DPA policy and procedures.

All staff

27. All staff follow SIC's data protection policy and procedures. They familiarise themselves with the implications of data protection in their job and keep personal data secure.

Appendix 1: Data Protection Principles

Schedule 1 to the DPA lists the data protection principles in the following terms:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless

    (a) at least one of the conditions in Schedule 2 is met, and

    (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. Personal data shall be 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.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under [the DPA].

7. Appropriate technical and organisational measures shall 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 shall 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.

Document control sheet

Document Information	
Full name of current version: Class, Title, Version No and status. *E.g. C1 MOU Between the SIC and the IC v0*	C5 Data Protection Policy and Handbook v01 CURRENT ISSUE
INVU No.	INV45232
Type	Policy & Procedure
Name of document in website file library	DataProtectionPolicyandHandbook
Approval	
Approver *(SMT, HOE, HOOM, HOPI)*	SMT
Approval Date	28/01/2014
For publication *(Y/N)*	Y
Review	
Responsible Manager (*SIC, HOE, HOOM, HOPI)*	HOOM
Date last major review	N/A
Date of last minor review	25/10/18
Date of next regular review	December 18
Publication	
Date published	25/10/18
Date guide to information updated	25/10/18
Action by *(initials)*	KB

Summary of changes to document				
Date	**Action by** *(initials)*	**Version updated** *(e.g. 01.25-36)*	**New version number** *(e.g. 01.27, or 02.03)*	**Brief description** (*e.g. updated paras 1-8, updated HOPI to HOOM, reviewed whole section on PI test, whole document updated, corrected typos, reformatted to new branding*)
29/01/14	KB	01.01	01.02	DCS updated, published on website
04/03/14	KB	01.02	01.03	DCS updated, remove reference to 'draft'
04/03/14	KB	01.03	01.04	DCS updated, date updated version published on Guide to Information
16/10/14	DL	01.04	01.05	Minor revision – tracked changes: Para 10 inserted re posting of sensitive personal data Para 18 inserted 'Breaches and near-misses' Enquiries Procedures – INV ref & hyperlink updated
16/10/14	DL	01.05	01.06	Changes accepted - DL
16/10/14	DL	01.06	01.07	Further refinement to Paras 18 & 18 – Breaches & near-misses
24/01/15	RA	01.07	01.08	VI updated
03/02/15	KB	01.08	01.09	Document title updated
03/02/15	KB	01.09	01.10	DCS updated, document published
22/02/18	KB	01.10	01.11	DCS updated, published on website
22/02/18	KB	01.11	01.12	Opened in edit mode in error, no changes made
25/10/18	KB	01.12	01.13	Review date amended, published on website

Scottish Information Commissioner
Kinburn Castle
Doubledykes Road
St Andrews, Fife
KY16 9DS

t 01334 464610
f 01334 464611
enquiries@itspublicknowledge.info

www.itspublicknowledge.info