Information and Records Management Policy

Scottish Information Commissioner

Contents

Glossary and abbreviations

Term used	Explanation
The Commissioner	The Scottish Information Commissioner
EIRS	Environmental Information (Scotland) Regulations 2004
FOISA	Freedom of Information (Scotland) Act 2002
SIC	The Scottish Information Commissioner, staff of SIC (depends on context)
The Section 61 Code	Scottish Ministers' Code of Practice on Records Management by Scottish Public Authorities under the FOISA
DPA	Data Protection Act 1998
PRSA	Public Records (Scotland) Act 2011
HOCS	Head of Corporate Services
RMT	Records Management Team

Section 1 - Information and Records Management Policy

Policy Statement

1. The Scottish Information Commissioner (SIC) recognises the value of our records as a corporate asset, and records management as a key corporate function. Our records are our corporate memory providing evidence of actions and decisions and supporting our daily functions and operations.

2. This policy and its related procedures and guidance are written with the intention of ensuring that adequate records are held by the SIC, can be accessed easily and quickly and that they are managed and controlled effectively, efficiently and economically and in support of our legal, operational and information needs.

Scope

3. Every member of staff employed by the SIC must comply with this Information and Records Management Policy and all related procedures and guidance.

4. A record is defined as "information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business"[1].

5. This policy covers all records held by the SIC regardless of format. This policy therefore covers records in the following formats:

    i. Audio and video tapes, cassettes

    ii. Email (including SIC information held in personal email accounts)

    iii. Facsimile (Fax)

    iv. Photographs

    v. Records in all electronic formats, including discs and CDs

    vi. Records in paper format.

6. This policy also covers all records in the above formats that have been transferred to the SIC by external organisations, for the duration of time that they remain in the care of the SIC.

7. The policy and its related procedures and guidance stipulate:

    i. The requirements that must be met for the records themselves to be considered as proper records of activity.

    ii. The systems and processes required to ensure the capture, integrity, security, retrievability and correct disposal of the SIC's records.

    iii. Staff responsibilities.

[1] International Standards Organisation ISO 15489 Information and documentation: Records Management, Part 1 2001

iv. Provision for regular review of the policy and its implementation.

Policy Objectives

8. The PRSA places an obligation on named authorities in Scotland, including the SIC, to produce a records management plan which sets out their arrangements for the effective management of all records.

9. This policy and its associated guidelines are intended to ensure that all records held by the SIC are effectively managed throughout their life cycle, from planning and creation through to ultimate disposal and meet the requirements of the PRSA. The eight main objectives of this policy are:-

    i. **Accountability** - that adequate records are maintained to account fully, transparently and accurately for all actions and decisions, and in particular:

        a. To facilitate audit or examination

        b. To provide credible and authoritative evidence

        c. To protect legal and other rights of staff, or other people affected by those actions

        d. To allow public access to information about:

            i. the services provided by the SIC

            ii. the costs of those services

            iii. the standard attained by those services

            iv. the facts which form the basis of decisions taken by the SIC which are of importance to the public

            v. the publication of reasons for decisions made by the SIC.

    ii. **Review and disposal** – that there are consistent and documented retention, selection and disposition procedures for deciding and managing the long term future of the various categories of records held by the SIC.

    iii. **Compliance** – that records comply with any record keeping requirements resulting from legislation including our duties as a data controller as defined by the DPA, audit rules and other relevant regulations, including the Section 61 Code.

    iv. **Performance measurement** – that the application of records management procedures are regularly monitored and reviewed, and action taken to improve standards as necessary

    v. **Retrievability** – that records and the information within them can be efficiently retrieved by those with a right of access, for as long as the records are held by the SIC

    vi. **Quality** – that records are complete and accurate and the metadata they contain is reliable and its authenticity can be guaranteed

    vii. **Security** – that records are secure from unauthorised or inadvertent alteration, destruction or deletion, that access and disclosure will be properly controlled and

audit trails will track all use and changes. Records and the systems in which they are held will be held in a robust format ensuring records remain retrievable and readable for as long as records are required.

viii. **Training** – that all staff are made aware of their record-keeping responsibilities through generic and specific training programmes and guidance.

Related Procedures and Guidance

10. This Information and Records Management Policy is supported by related procedures and guidance documents:
    i. Information and Records Management Handbook
    ii. File Plan and Retention Schedule
    iii. Records Review Procedures
11. The SIC has a Key Document Handbook and a Register of Key Documents is maintained.
12. In addition there are several policies and procedures whose main subject is not records management but which stipulate records management requirements specific to that subject, e.g. the Investigations Handbook and Employee Handbook.

Section 2 - Review, Retention and Disposal

13. The SIC's records Retention Schedule and related procedures set out the arrangement for managing review and recording the final disposal decisions for the SIC records when they cease to be active and come to the end of their useful life.

14. The schedule groups records according to the SIC functional file plan and is an essential component of efficient and effective records management, which must be consistently implemented by the SIC staff and regularly reviewed to maintain the integrity of the retention guidance. Implementation of this guidance will:-

    i. Ensure that the correct records are held by the SIC for the:

        a. conduct of business

        b. maintenance of corporate memory

        c. development of a knowledge base of skills and experience.

    ii. Support the SIC Records Management policy by providing appropriate guidance for authoritative and auditable disposal decisions and actions.

    iii. Assist in identifying records that may be worth preserving permanently as part of the SIC's archives.

    iv. Prevent the premature destruction of records that need to be retained for a specified period to satisfy legal, financial and other requirements of public administration.

    v. Provide consistency for the destruction of those records not required permanently after specified periods.

    vi. Avoid the costs and potential liabilities of retaining information the SIC does not need and may lead to non-compliance with the FOISA, the EIRs and the DPA and possible legal action against the organisation.

    vii. Ensure accurate indexing of records.

15. Nominated "Records Custodians[2]" are responsible for authorising or rejecting the disposal of any records which have been identified for destruction.

16. The HOCS will nominate a member or members of the RMT to meet annually with each Head of Department. They will ensure that the functional file plan and the associated records retention schedule remain current, and are amended as appropriate to reflect any changes to the information held e.g. following the commencement of a new activity.

[2] A named custodian (role) who is responsible for carrying out specific RM processes for categories of records e.g. record review. The Retention Schedule lists custodians of record categories.

Section 3 - Roles and Responsibilities

17. The Scottish Information Commissioner has overall responsibility for ensuring that records are managed responsibly within the SIC, and has delegated the management of this to the Head of Corporate Services (HOCS). These records management responsibilities are specified in the HOCS job description.

18. The HOCS is supported by a Records Management Team (RMT) which comprises representatives from across the SIC. The key responsibilities of the HOCS and the RMT are to:

    i. ensure that the SIC complies with the Section 61 Code and associated legislation

    ii. review and update this policy and associated guidelines to ensure they continue to support the records management requirements of the SIC in the undertaking of its operational and statutory functions

    iii. receive and approve change requests to the SIC information management system procedures and information structure

    iv. update these systems and issue update alerts to all staff

    v. arrange for the annual review and disposal of files

    vi. manage the audit programme and ensure any corrective actions are carried out

    vii. provide appropriate training, guidance and feedback mechanisms to support staff in carrying out their records management responsibilities.

19. It is the responsibility of all staff to ensure that they keep appropriate records of their work in the SIC and manage those records in keeping with this policy and associated procedures and guidance.

Training and Support

20. Staff training and support is recognised by the SIC as a pre-requisite to the successful implementation of its Information and Records Management policy. To this end appropriate training and guidance is provided to all staff:

    i. Information and Records management is included in the induction training programme

    ii. An annual training session reminding all staff of their responsibilities as set out in the Related Procedures and Guidance documents detailed above. These documents will be circulated to all staff annually, and staff must sign to confirm they have read and understood their contents.

    iii. The HOCS and members of the RMT will provide ongoing guidance to all staff on, and support with, record-keeping standards and procedures.

Section 4 - Performance Review and Compliance Monitoring

21. This Information and Records Management Policy is supported by a performance monitoring and compliance audit programme. The programme will:

    i. Monitor compliance with the policy and associated procedures

    ii. Put in place corrective actions and improvement processes to resolve any issues and areas of non-compliance identified during the monitoring and audit process.

22. The electronic document and records management systems used by the SIC log all records activity. This provides an audit trail which can be used as evidential support for system monitoring and compliance auditing.

23. The management and auditing of all the SIC information held in our electronic document and records management systems conforms with the recommendations in the Codes of Practice for evidential weight and legal admissibility of electronic information, BS 10008:2008.

24. The SIC's Governance Arrangements require a report on records management to be made annually to the senior management team. The purpose of the report is to provide assurance that:

    i. SIC records are being managed in accordance with published policies and guidance

    ii. Records are being held for the appropriate time

    iii. Records are being destroyed at the appropriate time

    iv. Information is being held securely

    v. Personal data is being lawfully processed.

25. The SIC will undertake periodic information and records management system self-improvement audits. This will be undertaken using tools such as the Scottish Council on Archives, Archives and Records Management Services (ARMS) Quality Improvement Framework online toolkit.

Section 5 - Relevant Legislation and Regulations

26. The policy supports compliance with the following legislation and statutory guidance:-

    i. Freedom of Information (Scotland) Act, 2002 and the Scottish Ministers' Code of Practice on Records Management published under S.61 of the Act

    ii. Environmental Information (Scotland) Regulations 2004

    iii. Data Protection Act 1998

    iv. Electronic Communications Act 2000

    v. Public Records (Scotland) Act 2011

    vi. Equality Act 2010

    vii. Human Rights Act 1998

    viii. Management of Health and Safety at Work Regulations 1999

    ix. Health and Safety at Work etc. Act 1974

    x. Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995

    xi. Other legislation relating to the particular subject area of certain records.

27. The SIC aims to operate in accordance with the following best practice standards for recordkeeping:-

    i. International Standard on Records Management, BS ISO 15489

    ii. Codes of Practice for evidential weight and legal admissibility of electronic information, BS 10008:2008

    iii. Principles for Good Practice for Information Management, PD0010:1997

Section 6 - Information Security

Policy Statement

28. Information is a valuable asset. Business continuity is dependent on its integrity and continued availability. Therefore, steps will be taken to protect information assets from unauthorised use, modification, disclosure or destruction, whether accidental or intentional.

29. The SIC is committed to the secure use of information and information technology systems in order to protect the availability, integrity and confidentiality of the information under our control. The SIC undertakes to have in place procedures to protect the information under our control.

30. The SIC will use a risk-based approach when assessing and understanding the risks and will use physical, personnel, technical and procedural means to achieve appropriate security measures, including conducting 'penetration testing' annually . We will take into account developments in technology and the costs of implementation in order to achieve a level of security appropriate to the nature of the information and the harm which may result from a security breach.

31. You are subject to a duty to keep confidential information that is provided to the SIC to carry out our functions under FOISA and the EIRs, and may only disclose it with lawful authority. The SIC will provide guidance and training to staff to enable them to understand and carry out their responsibilities in respect of security. We will assess their integrity and identity before they are employed. We will monitor their compliance with their obligations with respect to security.

32. Under section 65 of FOISA, it is a criminal offence for a Scottish public authority (or for any person employed by, who is an officer of, or is subject to the direction of, the authority) to alter, deface, block, erase, destroy or conceal a record held by the authority if a request has been made for information contained in the record and the applicant is entitled to be given the information.

Information Access

33. All documents and records will be available to all the SIC staff unless there is reason to restrict access for the purposes of business, personal security and/or justifiable confidentiality.

34. Compliance with these procedures also extends to the SIC's contractors and as such this requirement should be included within the terms and conditions of contracts drawn up between the SIC and the contracting organisation.

35. The SIC has in place a comprehensive business continuity plan which is designed to protect and provide early access to the SIC records in the event of disaster or serious disruption to normal business.

Information Security

36. You must take all reasonable steps to ensure that you do not unnecessarily compromise the security of the SIC's ICT systems.

37. You must follow the procedures and controls within the Information and Records Management Handbook , the Policy on the Use of the Internet and Email (Section 12.5 of the Employee Handbook, and associated guidance to manage your systems and the information contained on your system.

38. The SIC's laptops are encrypted. When you are provided with a laptop you are responsible for the laptop and its contents.

39. You must take all reasonable steps to ensure that no viruses are transmitted by you to any third parties and to ensure that you do not knowingly allow a virus to affect the SIC computer systems.

40. You must only use a memory stick provided by OMT. You must comply with the guidance on the use of memory sticks provided in the Information and Records Management Handbook.

41. You are not permitted to download any software, audio files, games, etc. from the internet or to install or use any unauthorised software or hardware from home to use on the SIC network unless it has been approved by the HOCS.

42. You will be provided with an IT account allowing access to SIC network. The account is secured by a password which must be changed every 30 days and must comply with the password convention detailed in the Staff Manual, IT Section.

Paper Mail Management

43. You must follow the procedure for the secure logging and tracking of incoming and outgoing mail, as detailed in the Staff Manual.

44. You must follow the procedures for removing case files from the building and file security when outside the building, as detailed in of the Investigation Handbook.

45. When you remove non case file records from the office, you must take all reasonable steps to ensure they remain secure at all times, and maintain confidentiality at a level appropriate to the content of the material. Confidential information (e.g. records containing personal data) should be only be removed from the office exceptionally, and with the prior permission of the HOCS.

Document control sheet

Document Information	
Full name of current version: Class, Title, Version No and Status. *E.g. C5 Key Documents Handbook v01 CURRENT ISSUE*	C5 Information and Records Management Policy v01 CURRENT ISSUE
VC FileId	36244
Type	Policy
Approver	SMT
Responsible Manager	HOOM
Date of next planned review	March 2018
Approval & Publication	
Approval Date (major version)	23/08/13
For publication *(Y/N)*	Y
Date published	13/09/17
Name of document in website file library	InformationandRecordsManagementPolicy
Corrections / Unplanned or Ad hoc reviews (see Summary of changes below for details)	
Date of last update	06/07/17

Summary of changes to document

Date	**Action by** *(initials)*	**Version updated** *(e.g. v01.25-36)*	**New version number** *(e.g. v01.27, 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*)
30/08/13	KB	01.01	01.02	Update INVU numbers
30/08/13	KB	01.02	01.03	Remove watermark
21/11/13	KB	01.03	01.05	Update INVU numbers
10/12/13	DL	01.05	01.07	Minor revision approved - DL
15/01/14	KB	01.07	01.08	Update Document Control Sheet
28/09/16	DL	01.08	01.11	Update para 30 re penetration testing
10/01/17	KB	01.11	01.12	VI'd, amend reference from INVU to VC, correct typos
10/01/17	KB	01.12	01.13	Update VC numbers
10/01/17	DL	01.13	01.14	Changes accepted
13/01/17	KB	01.14	01.15	DCS updated, published on website
03/07/17	KB	01.15	01.17	Opened twice in edit mode in error, no changes made
06/07/17	KB	01.17	01.18	Amended CS to CST, corrected typos
12/09/17	KB	01.18	01.19	Amended review date
13/09/17	KB	01.19	01.20	DCS updated, 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