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 2018
PRSA	Public Records (Scotland) Act 2011
HOCS	Head of Corporate Services
FAM	Finance and Administration Manager
RMT	Records Management Team
CST	Corporate Services Team
UK GDPR	UK General Data Protection Regulation
ICT	Information and communications technology

Section 1 - Information and Records Management Policy

Policy Statement

1. The Scottish Information Commissioner (the Commissioner) recognises the value of our records as a corporate asset and records management as a key corporate function. Our records provide evidence of actions and decisions and support our strategic objectives and operational functions. Having effective records management arrangements also helps us to:

    - increase efficiency and effectiveness, delivering savings in administration costs
    - improve and develop service delivery
    - achieve business objectives and targets
    - ensure compliance with the Public Records (Scotland) Act 2011 and other legislative requirements, standards and codes of conduct
    - support transparency and open government
    - underpin business resilience

2. This policy and its Related Procedures and Guidance ensure that adequate records are held by the Commissioner, that records can be accessed easily and quickly and that they are managed and controlled effectively, efficiently and economically in support of our legal, operational and information needs.

3. For business continuity purposes, it may be necessary to provide temporary and interim policies and procedures to add to or amend the provisions set out in this policy, for example, when dealing with the impact of a pandemic. Staff will be advised where such temporary and/or interim policies and/or procedures are required and the reasons for them.

Who and what does this policy cover?

4. Every member of staff employed by the Commissioner must comply with this Information and Records Management Policy and the Related Procedures and Guidance.

5. The Public Records (Scotland) Act 2011 (PRSA) states that "public records", in relation to an authority, means[1]:

    - records created by or on behalf of the authority in carrying out its functions
    - records created by or on behalf of a contractor in carrying out the authority's functions
    - records created by any other person that have come into the possession of the authority or a contractor in carrying out the authority's functions.

6. For our purposes we define a record as

[1] Public Records (Scotland) Act 2011, Section 3(1)

- information created, received, and maintained as evidence and information by our organisation or by a member of the Commissioner's staff, in pursuance of our legal obligations or in the transaction of our business
- information created, received, and maintained as an asset of our organisation in pursuance of our legal obligations or in the transaction of our business

7. This policy covers all records held by the Commissioner and the Commissioner's office irrespective of format or of the technology used to create and store them or the type of information they contain and includes the following:
    - email (including information held in staff email accounts)
    - facsimile (Fax)
    - photographs
    - records in all electronic formats, including discs and CDs, films
    - records in paper format
    - audio files
8. This policy also covers all records in the above formats that have been transferred to the Commissioner by external organisations, for the duration of time that they are held by the Commissioner.
9. The policy and its Related Procedures and Guidance set out:
    - The requirements that must be met for the records themselves to be considered as proper records of activity
    - The systems and processes required to ensure the capture, integrity, security, retrievability and correct disposal of the Commissioner's 's records
    - Staff responsibilities
    - Provision for regular review of the policy and its implementation.

Policy Objectives

10. The PRSA places an obligation on named authorities in Scotland, including the Commissioner, to produce and submit a records management plan ("RMP") setting out proper arrangements for the management of the authority's public records to the Keeper of the Records of Scotland ("the Keeper") for their agreement[2].
11. To assist authorities in this process, the Keeper publishes a model RMP ("Model RMP") that has been produced in consultation with stakeholders. The latest version of the Model RMP was published in 2019. The Model RMP sets out 15 elements that the Keeper would expect an organisation to consider when creating its RMP. It is recognised that all the elements of the Model RMP might not apply; however, should this be the case, the Keeper will expect to see an explanation in support of the omission of that element from its RMP.

[2] PRSA, Section 1

12. The Commissioner's RMP[3] sets out the arrangements for the effective management of all records held by the Commissioner's office.

13. This policy and the Related Procedures and Guidance are intended to ensure that all records held by the Commissioner are effectively managed throughout the life cycle of each record, from planning and creation through to ultimate disposal and that records 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:

            - the services provided by the Commissioner
            - the costs of those services
            - the standard attained by those services
            - the facts which form the basis of decisions taken by the Commissioner which are of importance to the public
            - the reasons for decisions made by the Commissioner.

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

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

    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 Commissioner

    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 the records are required.

[3] Agreed by the Keeper in 2014

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

Related Procedures and Guidance

14. This Information and Records Management Policy is supported by related procedures and guidance set out in the following documents:

- Information and Records Management Handbook
- File Plan and Retention Schedule
- Records Review Procedures
- Key Document Handbook
- Register of Key Documents

15. 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, for example, the Investigations Handbook, the Data Protection Policy and Handbook and the Employee Handbook.

Section 2 - Review, Retention and Disposal

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

17. The Retention Schedule groups records according to the Commissioner's functional File Plan[4] :

- the File Plan provides a framework for a consistent approach to classifying records across the organisation regardless of format or physical location and is an essential component of our efficient and effective records management; and
- in conjunction with the Retention Schedule, is used to identify and retrieve records relating to the same function and activity anywhere in the organisation, irrespective of which department produces or receives them.

18. The Retention Schedule should be consistently implemented by the Commissioner's staff and regularly reviewed to ensure that the retention guidance is up to date, relevant and appropriate.

19. The Retention Schedule helps us to:

i. Ensure that the correct records are held by the Commissioner for the:
   a. conduct of business
   b. maintenance of corporate memory
   c. development of a knowledge base of skills and experience.

ii. Support the Commissioner's 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 Commissioner'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 that the Commissioner does not need and may lead to non-compliance with the FOISA, the EIRs, the DPA and the UK GDPR and possible legal action against the organisation.

vii. Ensure accurate indexing of records.

[4] The File Plan is structured in a three-tier hierarchy representing business functions, activities and sub-activities carried out within the function.

18. The Retention Schedule lists custodians of record categories and these custodians are responsible for carrying out specific records management processes for categories of records for example, record review and for authorising or rejecting the disposal of any records which have been identified for destruction. The Finance and Administration Manager (FAM) (assisted as required by a member of the Corporate Services Team (CST)) will meet annually with each Head of Department to discuss the functional file plan and the associated records retention schedule to ensure that they remain current, and are amended as appropriate to reflect any changes to the information held e.g. following the commencement of any new activity.

Destruction of records

20. The Commissioner has suitable arrangements in place for the destruction of records, in accordance with the Retention Schedule. Records of destruction are created and retained in accordance with the Retention Schedule. Provision is made for the secure destruction of paper waste, including confidential paper waste and the assured secure destruction of sensitive digital records. The arrangements also cover the assured secure destruction of hardware and back-up media used to store digital records.

21. The above arrangements are reviewed to ensure that they are appropriate and remain relevant in the light of any statutory requirements.

22. The destruction of personal data is in accordance with data protection law.

Section 3 - Roles and Responsibilities

23. The Scottish Information Commissioner has overall responsibility for ensuring that records are managed responsibly within the Commissioner's office, and has delegated the management of this to the Head of Corporate Services (HOCS).

24. The HOCS is supported by the FAM and the CST and, as regards data protection, by the GDPR Working Party. The key responsibilities of the HOCS are to:

    i. ensure that the Commissioner complies with the Section 61 Code of Practice and associated legislation

    ii. review and update this policy and the Related Procedures and Guidance to ensure they continue to support the records management requirements of the Commissioner in the undertaking of its operational and statutory functions

    iii. receive and approve change requests to the Commissioner's information management system procedures and information structure

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

    v. arrange an 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.

25. It is the responsibility of all staff to ensure that they keep appropriate records of their work and manage those records in keeping with this policy and the Related Procedures and Guidance.

Training and Support

26. Staff training and support is recognised by the Commissioner as necessary for the successful implementation of this policy. Appropriate training and guidance is provided to all staff and includes the following:

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

    ii. Staff will be asked annually to confirm they have read and understood this policy and the Related Procedures and Guidance.

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

    iv. The HOCS will arrange for any required training in records management to be provided to staff.

Section 4 - Performance Review and Compliance Monitoring

27. 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.

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

29. The management and auditing of all the Commissioner's 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 10008:2020.

30. The Commissioner's Governance Arrangements require the HOCS to provide an annual report on records management to the senior management team and to provide assurance that the Commissioner's information and records are being managed in accordance with published policies and procedures and, in particular that:

    - records are being destroyed at the appropriate time
    - records are held for the appropriate time
    - information is held securely
    - appropriate back-up arrangements are in place
    - personal data is being lawfully processed
    - key documents are being managed in line with the Handbook

31. The Commissioner will undertake periodic information and records management system audits[5].

[5] For example, using tools such as Scottish Council on Archives, Archives and Records Management Services (ARMS) Quality Improvement Framework online toolkit.

Section 5 - Relevant Legislation and Regulations

32. 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 Section 61 of the Act

    ii. Environmental Information (Scotland) Regulations 2004

    iii. Data Protection Act 2018 and UK GDPR

    iv. Public Records (Scotland) Act 2011

    v. Equality Act 2010

    vi. Human Rights Act 1998

    vii. Management of Health and Safety at Work Regulations 1999

    viii. Health and Safety at Work etc. Act 1974

    ix. Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013

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

Freedom of Information

33. The Scottish Information Commissioner is responsible for enforcing and promoting freedom of information (FOI) law in Scotland which includes:

- Freedom of Information (Scotland) Act 2002 (FOISA)
  An Act of the Scottish Parliament which gives everyone the right to ask for any information held by a Scottish public authority.

- Environmental Information (Scotland) Regulations 2004 (the EIRs)
  The EIRs come from a European Directive on access to environmental information. The EIRs give everyone the right to ask for environmental information held by a Scottish public authority (and some other bodies).

- INSPIRE (Scotland) Regulations 2009
  These regulations also come from a European Directive, and require Scottish public authorities to make spatial datasets (e.g. map data) available.

34. The Commissioner holds and processes information and records related to applications made to the Commissioner and the Investigations Handbook sets out how this information and these records will be managed.

Data protection

35. The Commissioner holds and processes personal data about stakeholders, employees and contractors and is legally obliged to protect that information. Under data protection law, the Commissioner only collects information needed for a specific business purpose, keeps that

information secure, ensures it remains relevant and up to date, only holds information for as long as is necessary and enables subject access on request, unless an exemption applies.

36. The Commissioner has in place appropriate technical and organisational measures which include:

- a comprehensive data protection policy
- the appointment of a data protection officer
- procedures for the management of data breaches
- procedures to ensure that data protection impact assessments are carried out.
- a Privacy Notice to ensure that the Commissioner is as transparent as possible about the processing of personal data and enables individuals to determine what information the authority holds about them, how it is used, how long it is held and how they can exercise their rights.

Record Keeping

37. The Commissioner aims to operate in accordance with the following best practice standards for record keeping:-

i. International Standard on Records Management, BS ISO 15489

ii. Codes of Practice for evidential weight and legal admissibility of electronic information, BS 10008:2020

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

Section 6 - Information Security

Policy Statement

38. Information is a valuable asset and business continuity is dependent on its integrity and continued availability and the Commissioner 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.

39. Various improvements arising from a security review which took place in 2015-16 have been implemented and security was further reviewed as part of GDPR implementation in 2017-19.

40. There are processes and procedures in place to protect the information under our control and to protect information assets from unauthorised use, modification, disclosure or destruction, whether accidental or intentional. The Commissioner's information security procedures also take account of data protection and freedom of information obligations as well as any specific legislation or regulatory framework that may apply to the retention and security of records. The Commissioner uses a risk-based approach when assessing and understanding the risks and will use physical, personnel, technical and procedural means to achieve appropriate security measures in our IT systems, including conducting appropriate tests when required. The Commissioner also holds Cyber Essentials and Cyber Essentials Plus accreditations and will seek to renew these on an annual basis. We also take account of developments in technology, advice from technical experts 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 an information security breach.

41. When working remotely, all members of staff are still bound by our requirements regarding the security of information and must still comply with this policy and the key document C5 Information and Records Management Handbook.

42. All members of staff are subject to a duty to keep confidential information that is provided to the Commissioner to carry out our functions under FOISA and the EIRs, and may only disclose it with lawful authority[6]. The Commissioner will provide guidance and training to staff to enable them to understand and carry out their responsibilities in respect of information security. All members of staff have to be security cleared and we will monitor compliance with the obligations relating to information security.

43. All members of staff are made aware that 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.

[6] It is a criminal offence for the Commissioner and the Commissioner's staff to disclose information without lawful authority – Section 45 of FOISA. The DPA also contains a number of criminal offences regarding the misuse of personal data – Sections 170 to 173

Information Access

44. Generally, all documents and records are available to the Commissioner's staff unless there is reason to restrict access for the following reasons:

    - business purposes
    - employment and human resources purposes,
    - data protection requirements
    - personal security
    - confidentiality
    - a decision has been made to restrict access on the grounds that an exemption(s) in FOISA/an exception(s) in the EIRs would apply to that record if a request were to be made for the information.

45. Compliance with this policy also extends to the Commissioner's contractors and this requirement should be included within the terms and conditions of contracts entered into between the Commissioner and the contracting organisation/party.

46. We have in place appropriate security measures to prevent personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed

Business continuity

47. The National Records of Scotland Model Records Management Plan (Revised 2019), Element 10 advises that best practice might include:

    - An authority's business continuity arrangements should recognise the importance of the recovery of records.
    - Vital records are identified, perhaps as part of an Information Asset Register (see element 4), and the mechanisms for their protection and recovery included within the authority's Business Continuity Planning.
    - Arrangements are in place within the Plan that ensures that copies of vital records will both survive envisaged incidents and be available thereafter in accordance with defined criteria.
    - Arrangements are in place to ensure the ongoing confidentiality, integrity, availability and resilience of records involving personal data.
    - The authority's business continuity arrangements are reviewed regularly.

48. The Commissioner has a comprehensive business continuity plan which recognises the importance of the recovery of records and, also, is designed to protect and provide access to the Commissioner's records in the event of disaster or serious disruption to normal business.

49. In the event that business continuity arrangements are initiated, temporary records management procedures and guidance may be put in place to ensure that records are managed appropriately and in accordance with the relevant requirements whilst the business continuity arrangements are in place.

Archiving and transfer arrangements

50. The Commissioner has entered into a MOU with the Keeper to ensure that that records of enduring value and/or which are suitable and require permanent preservation are deposited in an appropriate archive repository. The Commissioner's Retention Schedule identifies records of enduring corporate and legal value. The MOU with the Keeper will be kept under review and update as necessary.

Information Security

51. Each member of staff must take all reasonable steps to ensure that they do not unnecessarily compromise the security of the Commissioner's ICT systems and records management systems.

52. Each member of staff must follow the procedures and controls within the Information and Records Management Handbook and the Principles on the Use of the Internet and Email (Part 2, Section 5 Professional Conduct of the Employee Handbook), and any other associated guidance which has been issued relating to the management of systems and the information contained on those systems.

53. Each member of staff is provided with a laptop which is encrypted and is responsible for the laptop and its contents and must:

- take all reasonable steps to ensure that no computer viruses or malware are transmitted to any third parties
- take all reasonable steps to ensure that no computer virus or malware affects the Commissioner's ICT computer systems.
- only use a memory stick provided by CST and comply with the guidance on the use of memory sticks provided in the Information and Records Management Handbook.
- not download any software, audio files, games, etc. from the internet or to install or use any unauthorised software or hardware to use on the Commissioner's network unless it has been approved by the HOCS.
- comply with all instructions which have been provided by the HOCS and/or the CST concerning the use of their work IT account, including any password policy.

Paper Record Management

54. All members of staff must follow the procedure for the secure logging and tracking of incoming and outgoing mail, as detailed in the Staff Manual.

55. All members of staff must follow the procedures for removing Enforcement case files (or extracts of case files) from the building and file security when outside the building, as detailed in of the Investigation Handbook.

56. When members of staff remove records relating to files other than Enforcement case files from the office, they 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 and personal data in files, other than Enforcement case files, 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 v02 CURRENT ISSUE
VC FileId	153689
Type	Policy
Approver	SMT
Responsible Manager	HOCS
Date of next planned review	March 2022
Approval & Publication	
Approval Date (major version)	30/06/21
For publication *(Y/N)*	Y
Date published	30/06/2021
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	

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*)
30/06/21	BOW	02.00	02.01	New document created following approval of draft
30/06/21	BOW	02.01	02.02	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