Information Management Policy

Document name	Information Management Policy
Version number	5.0
Status	Published
Department/Team	Information Management & Compliance
Relevant policies	All Information Management Policies and Guides
Distribution	Internal and External
Author/Owner	Information Management & Compliance
Approved by	Head of Cyber Security
Date of sign off	November 2020
Review by	01/02/2026
Security classification	Official

Key messages

This policy outlines the ICO's approach to information management at a high-level. The policy covers:

- Roles and responsibilities
- Managing risks to information
- Protection of personal data
- Storage, retention and disposal of information

Does this policy relate to me?

This policy relates to all ICO staff.

Table of contents

1. Introduction

1.1. This high-level policy sets out our commitment to following good information management practices. Our approach is guided by the section 46 Code of Practice on the Management of Records (the Code) and is based on the principles articulated in the Code.

1.2. In writing this policy, we've considered the nature of the information we hold, the work we do and the legal requirement for confidentiality imposed on the Commissioner and his staff.

1.3. Effective information management helps to ensure we have the right information at the right time to make the right decisions. We are committed to service excellence and information management is

vital to the delivery of our services in an orderly, efficient, and accountable manner.

1.4. Our information is a valuable corporate asset, and our records provide evidence of what we do and why. We aim to balance our commitment to openness and transparency with our responsibilities as an effective regulator. We know what information we hold, why we hold it and we manage information according to its sensitivity. We create and manage records efficiently, make them accessible where possible, protect and store them securely and dispose of them safely at the right time.

1.5. We only use corporate channels to process and store corporate information in line with our acceptable use policy. If we use non-corporate communication channels (NCCCs) for official purposes ie in emergencies, we transfer and store any relevant official information or record on to the corporate systems as soon as possible. Corporate information on NCCCs is caught by the Freedom of Information Act.

1.6. We have the appropriate governance, organisational capacity, and technical measures in place to manage information in accordance with the Code.

1.7. By adopting this policy, we aim to ensure that information, whatever form it takes, is accurate, reliable, ordered, complete, useful, up to date and accessible whenever it is needed to:

- help us carry out our business,
- help us to make informed decisions,
- protect the rights of our employees, the public and those we regulate,
- track policy changes and development,
- make sure we comply with relevant legislation,

- provide an audit trail to meet business, regulatory and legal requirements,
- make sure we have the essential tools to search, identify, locate and retrieve information,
- make sure we work effectively as a regulator and prosecuting authority and meet our lawful obligations for disclosing evidence in relation to Public Inquiries or legal action,
- support continuity and consistency in management and administration,
- make sure we are open, transparent, and responsive,
- support the maintenance of our publication scheme,
- support research and development; and
- promote our achievements.

1.8. This policy together with associated guidance and procedures applies to the management of all information, in both digital and physical formats, created or received by us. It applies to all staff, contractors, consultants and third parties who are given access to our documents and information processing facilities.

Back to Top

2. Statutory Framework

2.1. This policy provides a framework for meeting our information management responsibilities under relevant legislation, guidance and codes of practice including the:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018 (DPA 2018)
- Freedom of Information Act 2000 (FOIA 2000)
- Public Records Act 1958 (PRA 1958)
- Re-use of Public Sector Information Regulations 2015

- Section 46 Code of Practice on the management of records
- ICO's code-of-conduct

Back to Top

3. Roles and Responsibilities

3.1. All staff have a responsibility to ensure we manage our information and any associated risks appropriately and in accordance with this policy and its associated guidance and procedures.

3.2. To ensure that responsibility for delivering good standards of information management practice is embedded throughout the organisation we have an Information Risk Management Network (*internal link*) that assigns specific roles to individual staff. We provide these staff with specific guidance covering their role and their responsibilities (*internal link*). In summary, the membership of the network is as follows:

- Data Protection Officer (DPO)
- Senior Information Risk Owner (SIRO)
- Information Asset Owners (IAOs)
- Information Asset Managers (IAMs)
- Local Information Management Officers (LIMOs)
- SharePoint Site Owners (SOs)

3.3. Our SIRO is our Deputy Chief Executive and Chief Operating Officer and our IAOs are our Directors. Our DPO sits on our risk and compliance committees. Our Information Risk and Governance Group (IRGG) is concerned with ensuring that risk to information is appropriately managed.

3.4. Central support to the Information Risk Management Network is provided by several teams at the ICO with responsibilities and appropriate skills to deliver the following functions: Information Management, Information Security, Risk Management, Information Access, Facilities, IT teams, Legal teams, Procurement, and People Services .

3.5. The compliance teams also produce various policies, procedures and guidance and make them available to all staff in a central corporate repository.

3.6. A group manager heads the information management and compliance team. This team is responsible for the day-to-day management of ICO information and for producing policies, procedures and guidance.

Back to Top

4. Managing Risk to Information

4.1. Information Risk and Governance Group (IRGG) is responsible for the overview and scrutiny of information governance (IG) arrangements and for making recommendations to the Senior Information Risk Owner (SIRO) on information governance with data protection and compliance decisions as required. Issues from IRGG are escalated through the relevant Director/Executive Director to the Delivery and Regulatory group for decision if needed.

Back to Top

5. Protection of Personal Data

5.1. The ICO's Data Protection Policy provides a framework for ensuring that the ICO meets its obligations under the UK GDPR and the DPA 2018. It applies to all the processing of personal data carried out by the ICO including processing carried out by joint controllers, contractors, and processors.

Back to Top

6. Storage of Information at the ICO

6.1. We store our information in prescribed locations, appropriate to its format, content and sensitivity. We ensure appropriate controls are in place to maintain the confidentiality, integrity and availability of our information.

6.2. We have a storage policy (*internal link*) in addition to procedures and guidance to support staff to choose the right place to store information.

Back to Top

7. Security of Our Information

7.1. We ensure the security of our information via the implementation of a number of policies, procedures and guidance. Our Information Security Policy (*internal link*)supported by our Information Classification Guidance (*internal link*)ensures that information within our care receives an appropriate level of protection including access and permission control. Our staff use our systems in line with our Acceptable Use Policy (*internal link*) and Device Guidance (*internal link*).

Back to Top

8. Retention and Disposal

8.1. Our Retention and Disposal Policy outlines our approach to managing the retention and secure disposal of our information. It provides for a consistent approach and applies to all physical and digital information, regardless of storage location.

8.2. Our retention periods are driven by legislation or business need. If there is no legally defined retention period for corporate information, it is the responsibility of the relevant IAO (with input from the Information Management & Compliance team) to determine an appropriate retention period.

Back to Top

9. Appraisal and Selection for transfer to The National Archives

9.1. We follow our appraisal and selection methodology. The methodology describes how the ICO will meet its statutory obligation as a public record body under the terms of the PRA 1958. The methodology is supported by TNA training and guidance and ICO guidance.

Back to Top

10. Additional Policies and Training

10.1. This policy is supported by additional Information Management policies and guides that provide more detailed and subject-specific information to further its objectives. It is also supported by training such as the ICO's Information Governance training.

Back to Top

11. Monitoring and Compliance

11.1. Ongoing monitoring of compliance with this policy and its supporting policies, guidance and procedures will be undertaken on a regular basis by the Information Management Service and those with assigned responsibilities under the Information Risk Management Network (*internal link*). Monitoring compliance will also be supported by internal checks from the risk and compliance manager and external audits as appropriate.

Back to Top

Feedback on this document

If you have any feedback on this document, please fill in this feedback form (*internal link*).

Back to Top

Version history

Version	Changes made	Date	Made by
0.1	First Draft	20/11/2020	Ben Cudbertson
0.2	First Draft	23/11/2020	Iman El Mehdawy
1.0	Published	24/11/2020	Ben Cudbertson

Version	Changes made	Date	Made by
2.0	Major revision	06/06/2022	Iman El Mehdawy
2.1	Content moved to new template, minor formatting changes	09/09/2022	Ben Cudbertson
3.0	Review and addition of removable media and mobile devices link	01/02/23	Iman El Mehdawy
3.1	Formatting changes to meet accessibility requirements	24/03/2023	Ben Cudbertson
4.0	Annual review. 7.1 Link to Removable Media Guidance removed and amended link to Device Guidance	01/02/2024	Rosie Simpson
4.1	New entry at 1.5 added relating to the use of non-corporate communication channels	05/06/2024	Simon Lochery
5.0	Changes to add IRGG and service delivery group and remove RGB	15/01/2025	Iman El Mehdawy

Back to Top