Storage Policy

Version number: 5.0.

Status: Published.

Department/Team: Data and Information Management.

Relevant policies: Retention and Disposal Policy.

Distribution: Internal.

Author/Owner: Data and Information Management team.

Consultees: N/A.

Approved by: Iman Elmehdawy, Group Manager.

Application date: 06/09/2022.

Review date: 06/09/2027.

Security classification: Official.

Key messages

The main objective of this policy is to provide guidance on the storage of information at the ICO. The policy covers:

- storage of physical information;
- storage of digital information;
- storage of information off-site; and
- remote working.

Does this policy relate to me?

This policy applies to all ICO staff.

Table of Contents

1. Introduction

It is important to store our corporate information in the correct location, appropriate to its format, content, and sensitivity. Any location that is used to store corporate information (either physical or digital) must have information management controls in place.

Storing information correctly ensures we can keep track of it, and that it is accessible and quickly retrievable. We can also apply the appropriate retention and disposal schedule to it, as well as protect it from harm, unauthorised access, or degradation.

We have limited storage space for physical and digital information, therefore redundant, obsolete, and trivial material should be regularly weeded and disposed of to ensure that space is used effectively. Our Retention and Disposal Policy provides more information.

Back to the top

2. Storage of physical information

Physical records include information contained on paper, as well as removable media such as USB sticks, audio tapes and CDs. It is important that physical information is stored in the right location, appropriate to its sensitivity. For guidance on what types of information should be stored in which location, please consult the Storing Physical Information Guidance (internal link).

Office Storage Space

Each team will have cupboards or filing cabinets in which to store their physical records. Each one will need:

- to be listed on the Storage Asset Register (internal link);
- to be assigned a unique reference number and Storage Asset Label. You can contact the Data and Information Management team if you do not have these; and
- to be assigned a key which is labelled with the cupboard's unique reference number. Facilities can replace lost keys.

The Storage Asset Register (internal link) should be used to record the location of a storage asset, its owner and the sensitivity of the asset's contents. It is not necessary to detail any information about the contents of the records.

It is the responsibility of the Local Information Management Officer (LIMO) to ensure that this register is kept up to date for the storage assets used by their team.

Each team should take care to ensure that the information contained in cupboards and cabinets is secure and information must not be left out on desks overnight. The keys to these cupboards should be stored securely in the office key cabinet. The code to the key cabinet should only be shared with those who require access.

If you are storing information in a safe which is accessed via a code, then the code should only be known by those who require access to the information. The code should be changed regularly.

Personal Lockers

Corporate information should not be stored in personal lockers. These should be reserved for personal items, or low-value, non corporate, information such as training notes or copies of legislation. Keys for personal lockers should be stored in the office key cabinet.

Off-site Storage

The ICO uses a third-party contractor for off-site storage. Departments should store information off-site if:

- they don't need to access it regularly (monthly); or
- it has been selected for permanent preservation; or
- it is too voluminous to store on-site.

The Off-site Storage Guidance (internal link) provides more information on how boxes are transferred to and from off-site storage. Please contact the Data and Information Management team if your team requires the use of off-site storage.

Remote Working

Authorisation should be obtained before any physical information is removed from the office. Physical information which is taken out of the office must be logged on the relevant team physical information tracking log before it is removed. A template Physical Information Tracking Log (internal link) is available for use and each team should have their own version saved locally into their SharePoint Online EDRM site.

Physical information which is taken home must be stored securely. If possible, the information should be locked away when not in use. Employees are bound by the ICO Code of Conduct to ensure any confidential information is not disclosed.

Printing at home is permitted in limited circumstances. Further information is in the Taking ICO information off site guidance (internal link).

Back to the top

3. Storage of digital information

Digital information includes any document which is stored on an ICO system or application, such as SharePoint Online EDRM, ICE or Microsoft 365.[1] It is important that digital information is stored in the right location, appropriate to its sensitivity. For guidance on which types of digital information should be stored in which location, please consult the What Digital Information to Save and Where Guidance (internal link).

SharePoint Online EDRM

Digital information that does need to be stored in a specific casework system should be stored on SharePoint Online EDRM. It is important for corporate information to be stored in a central location such as SharePoint Online EDRM so that it has the appropriate information governance controls in place. The exception to this is any private information you hold, for example, details of 121s with your manager, pay-related information, or your own training notes. This information should be stored on your OneDrive instead.

Each team should have their own site on SharePoint Online EDRM where their information should be stored. If you do not have anywhere to store your team's records on SharePoint Online EDRM, please contact IT Help. It is the responsibility of each team's Site Owners to manage the structure and organisation of the information within their SharePoint site.

Casework

All current casework should be stored in ICE where possible, including:

- ICE 360;
- ICE Registration; and
- ICE Interim.

[1] This includes Outlook, Teams and OneDrive.

Generally, casework should not be stored in SharePoint EDRM. However, there are exceptions for some Investigations teams who require the use of SharePoint EDRM for certain casework. If you're unsure, please check before saving casework to SharePoint EDRM.

Legacy casework will be stored in CMEH Legacy, where it will remain for the duration of its retention period.

Microsoft 365 Applications

Any information held in Microsoft 365 applications such as OneDrive, Outlook and Teams must only be stored there temporarily. Everyone is responsible for ensuring that all records that need to be retained are saved to SharePoint Online EDRM.

OneDrive: only your private information can be stored on OneDrive long-term. OneDrive may be used to temporarily store corporate information, such as initial drafts of documents, however once these have been uploaded to SharePoint Online EDRM the OneDrive copy must be deleted to avoid duplication.

Outlook: emails in Outlook have a retention period of 12 months, after which they will be automatically deleted. Any emails which need to be saved for longer must be saved into the appropriate system.

Teams: Microsoft Teams may be used for collaboration, for example drafting documents. It should not be used for long-term storage of information. Once the drafts have been finalised the documents should be saved into SharePoint Online EDRM and then deleted from Teams. Further guidance on Teams can be found in the Managing Information in Microsoft Teams Guidance (internal link).

Instant messages in Teams will be automatically deleted after seven days. We need to retain a record of any decisions which require sign-off or approval, therefore you should not use instant messaging through Teams for formal or high-level decision making. If decisions have been made using instant messaging, then this decision should be confirmed in an email and then saved into SharePoint Online EDRM in order to preserve an audit trail.

Corporate information should be stored in either SharePoint Online EDRM (non-casework) or ICE (casework) where possible, however there may be instances where corporate information needs to be stored in other systems across the ICO.

Any system which contains corporate information should have information management controls in place. It is best practice to ensure that for each system:

- redundant, obsolete, or trivial material is deleted;
- information is not kept beyond its retention period;
- there is a process in place for managing access;
- information can be securely and permanently deleted; and
- Accessibility is maintained. This may involve migration of information between environments and systems, conversion to current software versions, or conversion from obsolete to current file formats.

The ICO stores a high volume of digital information. In order to ensure it is possible to easily retrieve our documents, records should not be saved into any system unless they have been given a clear and logical file name in accordance with the ICO Naming Convention (internal link). Records with unclear file names are at risk of being lost.

Back to the top

Version history

Version	Changes Made	Date	Made by
0.1	First draft.	25/02/2022	Ben Cudbertson
1.0	Published.	04/03/2022	Ben Cudbertson

1.1	Teams instant messages retention period changed to seven days.	04/05/2022	Simon Lochery
1.2	Minor updates to clarify storage of PDRs, flexi sheets, and pay-related information.	14/06/2022	Ben Cudbertson
1.3	Content moved to new template, minor formatting changes.	06/09/2022	Ben Cudbertson
2.0	Annual review. 1.3 – minor change to paragraph contents. 2.1.2. & 2.1.3 - clarified purpose of Storage Asset Register.	03/02/2022	Steven Johnston
2.1	Formatting changes to meet accessibility requirements.	23/05/2023	Ben Cudbertson
3.0	Annual review, no changes.	21/01/2024	Rosie Simpson
4.0	Annual review. Changes made in section 3 to remove reference to storing PDR and flexi sheets in OneDrive and to clarify private information.	07/02/2025	Simon Lochery

4.1	Minor amendment to wording in section 3.1.1. Changes to section 3.2 to account for exception for some Investigations teams using EDRM for casework.	29/10/2025	Simon Lochery
5.0	Annual review. Minor content and formatting changes throughout to conform to new corporate template and style guide.	03/02/2025	Steven Johnston

Back to the top