Group policy

Information Management Policy

Version 1 | Public | June 2025

Contents

1 Overview 3

1.1 Introduction 3

1.2 Purpose 3

1.3 Who Must Comply 3

1.4 Core Principles 3

1.5 Policy Framework 4

2 Record Retention 5

2.1 Record Retention Schedules 5

2.2 Records in the public interest 5

2.3 Document weeding 5

2.4 Document preservation notices 6

3 Accountabilities, Roles & Responsibilities 7

3.1 Roles 7

2.1.1 Data Sponsor 7

2.1.2 Deputy Data Sponsor 7

2.1.3 Data Owner 7

2.1.4 Site Owner 7

4 Storage 8

4.1 Approved storage locations 8

4.2 OneDrive 8

4.3 Outlook 8

5 Where to go for help 9

5.1 Reporting Non-Compliance 9

5.2 Reporting a Concern – How to 'Speak Up' 9

6 Document control 10

6.1 Document control record 10

6.2 Policy Approval 10

Appendices 11

Definitions 11

Applicable regulation and legislation 12

Governance Responsibilities 13

1 Overview

1.1 Introduction

The Chief Financial Officer has overall accountability to the Post Office Group[1] Boards for the design and implementation of controls to prevent and manage the risks associated with information management.

1.2 Purpose

Post Office is committed to the efficient management of our information and records for the effective delivery of our services, to document our principal activities, and to maintain corporate memory. The purpose of this policy is to provide a consistent, coherent, and proportionate approach to information management. This is inclusive of physical and digital information.

This policy defines the Post Office approach to document and records management, including individual information management responsibilities, record retention and storage.

It is one of a set of policies which provide a clear risk and governance framework and an effective system of internal control for the management of risk across Post Office. Compliance with these policies supports the Post Office in meeting its business objectives and to balance the needs of postmasters, shareholders, employees, and other stakeholders.

1.3 Who Must Comply

Compliance with this policy is mandatory for:

- All employees[2] working within or for Post Office Limited, including permanent and temporary colleagues (consultants, contractors, third party agents and their employees).
- All Group legal entities, franchise partners and subsidiaries.

Where the Post Office holds a supplier relationship with a third party, and it is appropriate for the supplier to adhere to this policy then provisions should be included within their contracts to reflect this along with their own equivalent Policy.

1.4 Core Principles

The Post Office will:

[1] In this Policy "Post Office" and "Group" means Post Office Limited and its wholly owned subsidiary, Post Office Management Services Limited.

[2] In this Policy "employee" and "staff" means all persons working for the Group or on our behalf in any capacity including employees at all levels, directors, agency workers, volunteers, interns, and contractors.

a. Comply with all applicable legal and regulatory requirements that Post Office is subject to in relation to information management, reducing the risk of financial penalties, prosecution, or reputational damage.

b. Maintain an effective governance and assurance environment in respect of Information Management.

c. Foster an environment where information is proactively owned and managed throughout its lifecycle to aid with swift retrieval.

d. Comply with The Public Records Act 1958 and 1967 by preserving information that is in the public interest and contributes to the Post Office's story in society, supporting corporate memory and brand identity.

1.5 Policy Framework

The Information Management Policy (the "Policy") is reviewed and updated annually, or more frequently as necessary. This is to ensure its ongoing relevance and compliance with regulatory and legislative changes, as well as to reflect any lessons learned from both internal and external events.

This policy is classified as a Group Key Policy. It is therefore subject to annual review and endorsement at the Risk and Compliance Committee (R&CC), the Audit, Risk and Compliance Committee (ARC) and Board where appropriate. Thereafter, it is adopted by Post Office Limited and its wholly owned subsidary[3].

[3] This refers to Post Office Management Services Limited, which is an FCA regulated principal.

2 Record Retention

2.1 Record Retention Schedules

Information held for longer than is necessary carries additional risk and cost. Records and information should only be retained for as long as there is a business or legal requirement to do so. Under UK GDPR and the Data Protection Act 2018 personal data processed by Post Office must not be retained for longer than is necessary for its lawful purpose.

A record can be in any format (handwritten document, audio file, video file etc) and provides evidence or information about the past. It should not be edited or revised in any way because it may be used as evidence of legal obligations or in the transaction of business and editing it would prevent it from being a factual account of the event.

Post Office has Record Retention Schedules which outline the key records owned and managed by each business unit throughout their lifecycle. The schedules log –

- A description of the records.
- The location of the records.
- Whether any personal data is included, and the information classification of the records.
- The retention period and rationale. This retention period will vary depending on the type of record.
- The end of period action – Destroy, Review or Offer to Archive.
- Information on the Data Owner, Business Unit and Data Sponsor.

Records should be retained for the length of time defined in the schedule unless there is a legal requirement to destroy them sooner. Information may be retained for longer than is defined in the schedule, where there is a justifiable requirement to do so.

The Record Retention Schedules are reviewed on an annual basis, or when there is significant change.

2.2 Records in the public interest

Post Office is legally bound to archive certain records which are in the public interest, pursuant to the Public Records Acts 1958 and 1967. Post Office commits to assessing its records to transfer those eligible for preservation to the place of deposit appointed by the Secretary of State (The Postal Museum).

2.3 Document weeding

A high volume of information that Post Office creates and stores does not have long term business value, or any legislative requirement to be retained. Information such as draft documents, duplicates, documents used and saved to research topics, and those designed to keep track of daily activities

have limited to no long-term value. They should be deleted as soon as they are no longer required in order to:

- Ensure money is not wasted by storing information that is not needed, either digitally or physically.
- Reduce the volume of data which could potentially be impacted by any security breach, for example a cyber security incident.
- Ensure compliance with the Data Protection Act by retaining personal data only for as long as necessary.

All employees have a responsibility to weed documents they have created and saved.

Weeding should take place on a regular basis [remaining cognisant of any legal holds – refer to section 2.4] to prevent documents of limited value building up. When completed regularly, weeding can be completed relatively quickly as there will be recent knowledge of the content of the documents, and a simple assessment can be made of their ongoing value. It may be practical to agree a regular weeding schedule within each team based on available resource and volume of information generated.

Weeding should include documents stored in personal OneDrive accounts and desktops, and paper documents. Paper documents should be disposed of in accordance with the guidance in the Information Classification Standard (via confidential waste for internal, confidential or strictly confidential documents.)

2.4 Document preservation notices

Regulatory investigations, civil litigation or other legal matters may trigger a requirement for Post Office to preserve certain information and records, including documents, emails, and other digital data. In that event, Post Office's Legal Team will send a document preservation notice (or 'legal hold') to the custodians identified (whether individual staff members or business units) which may hold relevant information. This notice will provide guidance to the custodians about the steps required, which may include suspending end of period actions under the relevant Record Retention Schedules or routine deletion processes. All Post Office staff are expected to comply with any document preservation notices they may receive, until it has been confirmed that the legal hold has been removed.

Post Office is currently subject to a number of legal holds in relation to the Post Office Horizon IT Inquiry and other matters. The Post Office Legal Team can provide additional information on any legal holds that are in place at a given time.

3 Accountabilities, Roles & Responsibilities

3.1 Roles

All Post Office staff are responsible for managing the information they create and receive as part of their normal daily business activities (in both physical and digital format) and must manage it carefully and according to its information classification.

Post Office has defined specific information management roles which are delegated to colleagues across the business. The Data Management Team can advise on who these roles are assigned to at any given time.

2.1.1 Data Sponsor

Data Sponsors are accountable for the data and information within their business unit. This includes understanding what data and information is held, who has access to is, what is added and removed and why.

2.1.2 Deputy Data Sponsor

Deputy Data Sponsors are nominated by the Data Sponsor to co-ordinate data governance activities across their business unit, including co-ordinating the review of Record Retention Schedules within their business unit.

2.1.3 Data Owner

The person with responsibility for managing specific data and information within their business unit, and ensuring compliance with the POL Record Retention Schedules.

2.1.4 Site Owner

A site owner is responsible for the administration and access controls of the Microsoft Teams and SharePoint sites for which they are an 'owner.' They are responsible for –

- Ensuring there are always at least two owners of each site.
- Adding and removing members when necessary and appropriate, completing regular membership reviews to ensure continued access is warranted.
- Managing requests from non-members to access information held in the site, considering the appropriateness of sharing.
- Managing end of life sites in accordance with Post Office guidance.

4 Storage

4.1 Approved storage locations

The majority of Post Office information is created in a digital format, and business records should be stored in approved digital storage locations such as –

- Post Office SharePoint/Teams
- Approved databases/software systems.

Physical records should only be created where there is a specific requirement to do so. Any physical records should be stored and managed securely under the direction of the Data Owner until such time as they are transferred to archive storage. Physical **records** should not be stored at an employee's home address unless there is a legitimate need to do so, which is known and authorised by the Data Owner.

Physical **documents** such as print outs or hand-written notes containing Post Office information should not be stored at an staff member's home address unless there is a legitimate need, and should be disposed of as soon as practicable. It is the responsibility of the staff member to dispose of these documents in accordance with the guidance in the Information Classification Standard.

4.2 OneDrive

OneDrive accounts are provided to some Post Office staff members, and allow users to save, access and share files. Post Office enables its staff to store their personal files within their own OneDrive account. Post Office does not permit business records to be stored in OneDrive due to difficulties in access and retrieval, particularly once a user leaves the organisation. Where business records are stored in the OneDrive account of a staff member who has left the organisation, records can only be recovered via complex, time consuming technical searches and recovery, and for a limited period.

OneDrive accounts remain subject to legislation such as Freedom of Information and Data Protection. It is the responsibility of the account owner to ensure that business records are stored in the correct location and not duplicated.

4.3 Outlook

Microsoft Outlook is an application that is used mainly to send and receive emails. It is also used to manage calendar appointments, task managing and similar activities.

Post Office permits the use of Outlook to correspond internally and externally via email. Shared mailboxes are also permitted to facilitate correspondence which is directed to a team rather than a specific individual. Post Office does not permit business records to be stored in Outlook unless there is a legitimate need to do so, which is known and authorised by the Data Owner and reflective of any retention policies in place in Outlook. It is the responsibility of the owner of the account to ensure that any business records are transferred to an appropriate storage location for onward management where necessary.

5 Where to go for help

5.1 Reporting Non-Compliance

Where non-compliance is identified, the matter must be referred to the Policy Owner, which is the Interim Data Management Director. Where required, any investigations will be carried out in accordance with the Investigations Policy.

Where it is identified that an instance of non-compliance is caused through wilful disregard and / or negligence, this may be treated as a disciplinary matter.

5.2 Reporting a Concern – How to 'Speak Up'

Post Office strive to foster an environment where everyone feels comfortable speaking up. Post Office encourages anyone to raise concerns about wrongdoing, illegal activities, or unethical behaviour.
Information and contact details:
Confidential reporting Speak Up service:

- Telephone Number: 0800 041 8159
- http://speakup.postoffice.co.uk/ which is a secure on-line web portal
- Via email: speakup@postoffice.co.uk

6 Document control

6.1 Document control record

Summary

Version	Document review period	Policy – effective date	Policy location
1.0	Annual	June 2025	https://corporate.postoffice.co.uk/en/governance/our-structure/useful-corporate-information/

6.2 Policy Approval

Committee	Date approved
POL R&CC	**16/06/2025**
POL ARC	**NA**
POMS ARC	**29/07/2025**

Next policy annual review date: June 2026

Appendices

Definitions

1. POL Record Retention Schedules – These schedules document the types of record that each business unit hold, how long they should hold them for and what action to take when they are no longer required. Retention schedules set out the groups of records that Post Office functions will maintain and when these are due for review, transfer to The Postal Museum or secure destruction. Retention periods and actions are based on business value, evidential value, legal or regulatory requirements, and historical value.

2. Record – A record can be in any format (handwritten document, audio file, video file etc) and provides evidence or information about the past. They cannot be edited or revised in any way because they can be used as evidence in legal obligations or in the transaction of business and editing them would prevent them from being a factual account of the event.

3. Documents - a type of information which has been used to form the basis of decisions, record business obligations, or to support business processes, in the normal day to day running of Post Office.

4. Information – is defined as a collection of data in the form of documents or other artefacts (such as spreadsheets, flow diagrams or reports) on which the business makes decisions.

5. Physical information – information in a tangible physical format, for example paper, CDs, DVD's.

6. Digital information – information that exists in a digital or electronic format, for example computer files, database content.

7. Data - is defined as the elements that form part of systems and processes that are created or pass through our systems.

Applicable regulation and legislation

The following non-exhaustive list of legislation concerning the creation, management, disposal, use and re-use of documents and information is applicable to Post Office but please note that some legislation may be applicable only to some entities in the Group i.e. based on the services provided as at the date of this policy the Public Records Acts will only apply to Post Office Limited and not its subsidiary:

- Postal Services Act 2000
- Data Protection Act (2018)
- Freedom of Information Act (2000)
- Companies Acts (1985, 2006)
- Limitation Act (1980)
- Public Records Acts (1958)
- Financial Services and Markets Act (2000)

Governance Responsibilities

The Policy Sponsor responsible for overseeing this Policy is the Chief Financial Officer.

The Policy Owner is the Interim Data Management Director who is responsible for ensuring that the content is up to date and is capable of being executed. The Interim Data Management Director is responsible for providing appropriate and timely reporting to the Risk and Compliance Committee and the Audit and Risk Committee as required.

The Audit, Risk and Compliance Committee is responsible for approving the Policy and overseeing compliance.

Additionally, the Policy Owner will ensure that the policy is implemented in practice and will inform the owners of other impacted policies where new or significant changes are made to this policy.