POL00362761

GROUP POLICIES

Document Retention and Disposal Policy

Version – V1.2

POL00362761

1. Contents

1. Contents....2
2. Overview....3
2.1. Introduction by the Policy Owner....3
2.2. Risk Appetite....3
2.3. Purpose....3
2.4. Core Principles....4
2.5. Application....4
2.6. Definitions....4
2.7. Legislation....5
2.8. Industry Guidance....6
3. Minimum Control Standards....7
4. Tools – Retention Schedules....13
4.1. Functional Retention Schedules....13
5. Where to go for help....14
5.1. Additional Policies....14
5.2. How to raise a concern....14
5.3. Who to contact for more information....14
6. Control....15
6.1. Policy Version....15
6.2. Policy Approval....15

POL00362761

2. Overview

2.1. Introduction by the Policy Owner

This policy sets out Post Office's commitment to the proper and lawful retention and disposal of its Information Assets by the Group. Information held for longer than is necessary carries additional risk and cost. Conversely, information not kept for long enough leaves Post Office vulnerable to knowledge or evidence gaps and sanctions from some of our regulators. Post Office recognises that failure to follow these principles will negatively impact business efficiency, and the ability to protect its interests as well as those of its customers and stakeholders.

2.2. Risk Appetite

A Risk Appetite is the extent to which the group will accept that a risk might happen in pursuit of day to day business transactions. It therefore defines the boundaries of activity and levels of exposure that the group are willing and able to tolerate.

The Group takes its legal and regulatory responsibilities seriously and consequently has:

- **Averse** risk appetite in relation to not complying with law and regulations or deviation from its business conduct standards, of which this standard forms part
- **Averse** risk appetite in relation to any serious impact to the confidentiality, integrity and availability of information, leading to financial loss, business disruption, public embarrassment or legal consequences in line with risk impacts
- **Tolerant** risk appetite for legal and regulatory risk in those limited circumstances where there are significant conflicting imperatives between conformance and commercial practicality
- **Averse** risk appetite for litigation in relation to high profile cases/ issues
- **Averse** risk appetite for data loss/ leakage that can lead to customer, commercial or reputational damage
- **Averse** risk appetite for inaccurate and unreliable processing of data
- **Averse** risk appetite for inefficient or ineffective or prolonged failure of, governance and control processes, critical financial reporting processes, critical supply chain and business continuity processes.

2.3. Purpose

The Document Retention and Disposal Policy is a cornerstone for good information management in Post Office. Information management supports the delivery of Post Office services in an efficient and accountable manner, helping to maintain its position as a trusted provider, retaining information for operational use while ensuring adherence to the laws and regulations concerning them. The objective of this policy is to ensure that the Group complies with its legal obligations in respect of the retention and disposal of

POL00362761

Information Assets, keep important information for future use or reference, organise information so it can be searched and accessed at a later date and dispose of information that is no longer needed.

This policy defines a set of high level principles to manage the retention and disposal of Post Office's information Assets in a timely and secure manner according to business needs and legal and regulatory requirements.

All Employees have a responsibility to understand the requirements set out in this policy and seek clarification from their line manager or the Departmental Data Steward in the case of any uncertainty. A list of Data Owners and Departmental Data Stewards will be maintained on the Data Management area of the intranet and will be updated when staff change, or new ones are added. The address for the Data Management Site is: https://poluk.sharepoint.com/sites/Extranet/FandO/DG/Lists/Entities/AllItems.aspx

2.4. Core Principles

Compliance with this policy will assist in meeting the following principles:

- Information that is needed to minimise the risk to Post Office from investigations, litigation or disputes will be easier to locate and will be retained systematically.
- Employees will have clear guidelines for the secure disposal of information, protecting against misuse and data breaches.
- Information that contributes to the Post Office's story in society will be protected, supporting corporate memory and brand identity through heritage.
- Post Office is subject to many laws and regulations which have information retention requirements. Compliance with these requirements will significantly reduce the risk of financial penalties, prosecution or reputational damage.
- Properly managed retention and disposal of information will allow Post Office to defend its actions by evidencing document destruction. Retention schedules and destruction/transfer documentation will underpin auditable disposal processes. In particular, this will support compliance with the Freedom of Information Act and the Data Protection Act 2018.
- Timely disposal of information will lead to financial savings for document storage, as well as day to day efficiency savings when retrieving information.

2.5. Application

This standard applies to all Post Office staff and third-party's who have access to Post Office data especially those with elevated rights to Post Office data.

2.6. Definitions

Data

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

Data Entity

'Data Entity' is the term used to describe a concept in a data repository that is a container of data & relationships to other objects – such as Branch, Customer, Employee, Product etc.

POL00362761

Data Owner

'Data Owner' is the person (usually GE or GE-1) who is accountable for a data entity (or multiple data entities).

Departmental Data Steward

'Departmental Data Steward' is the person allocated by a Data Owner to undertake the day to day processes associated with the controls required by the Data Owner.

Document Retention Schedule

'Document Retention Schedule' is the document detailing the various requirements of the data owner in regard to documents under their sphere of control.

Documents

'Documents' are specifically a type of information which has been used to form the basis of decisions, or to support business processes, in the normal day to day running of Post Office.

Employee

'Employee' means employees permanent employees, temporary including agency employees, contractors, consultants and anyone else working on behalf of Post Office.

Group

'Group' refers to Post Office Limited and its subsidiaries.

Information

'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.

Information Assets

'Information Assets' are collectively the Information, Data and Documents.

Structured Data

'Structured Data' has pre-defined data models or schema within a database or system file.

Unstructured Data

'Unstructured Data' consist all those that do not have pre-defined data models or schemas thus can't be so readily classified and fit into a neat box. Unstructured data files often include text and multimedia content: photos and graphic images, videos, webpages, PDF files, PowerPoint presentations, emails, blog entries, wikis and word processing documents.

2.7. 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

POL00362761

only apply to Post Office Limited and not its subsidiaries (please note that the list below is not exhaustive and other legislation may apply):

- Postal Services Act 2000
- Data Protection Act (2018)
- Freedom of Information Act (2000)
- Companies Acts (1985, 2006)
- Limitation Act (1980)
- Public Records Acts (1958, 1967)
- Financial Services and Markets Act (2000)

2.8. Industry Guidance

This policy is based on the international standard for records management, ISO 15489 and the Code of Practice on the management of records under Section 46 of the Freedom of Information Act 2000.

POL00362761

3. Minimum Control Standards

A minimum control standard is an activity which must be in place in order to manage the risks so they remain within the defined Risk Appetite statements. There must be mechanisms in place within each business unit to demonstrate compliance. The minimum control standards can cover a range of control types, i.e. directive, detective, corrective and preventive which are required to ensure risks are managed to an acceptable level and within the defined Risk Appetite.

The table below sets out the relationships between identified risk and the required minimum control standards in consideration of the stated risk appetite. The subsequent pages define the terms used in greater detail:

At Document/System Creation

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
Product or service entity	Systems may not adequately support implementation of retention schedules and timely destruction of data. It may not be technically possible to permanently delete data or it may require a manual process.	As part of the design of a new product or service, or where a product or service is being updated, product or service risks must be considered, mitigated and documented before completion of design phase. This must include updating of any related Document Retention Schedules.	Product, Project and Programme Managers.	During design phase/ annually/ anytime there is a change
		The integrity and accuracy of data must be ensured at the point of collection.	Data Owner, Product, Project and Programme Managers.	During design phase/ annually/ anytime there is a change
Retention Schedules	Lack of creation or updating of retention schedules means that colleagues may not be aware of their obligations leading to	Data Owners are responsible for maintenance and adherence of their retention schedules. All Data Owners must ensure that the retention schedules for their area are up to date. This	Data Owner	All the time

POL00362761

	inappropriate usage or retention of documents. This can cause Post Office to be fined or suffer reputational damage.	is especially important when changes are being implemented to business processes.		

During Use of a document or system

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
Risks to Information	Lack of understanding of the importance or sensitivity of the information flowing through a department could mean that employees do not perform the required actions on it.	Data Owners must ensure that all employees who view or process the information within their sphere of control understand the importance of that data.	Data Owners	Every 6 months in the Director assertions. All the time
		Data Owners need to understand the designs of systems or products such that they can fully understand the scope of their entity. Data Owners may pass this to Departmental Data Stewards, but they retain accountability.	Data Owners	All the time
		Data Owners must ensure evidence of any decisions are retained.	Data Owners	All the time
		Data Owners must understand the complete information lifecycle (creation, capture, index, manage, access, retrieve, administer, repurpose, share, retain, dispose, preserve) for all data within their sphere of control.	Data Owners	All the time
Access Control	Inadequate access controls may lead to unauthorised deletion of information including sensitive or business critical information.	Line Managers must assess and assure risks relating to employee access to systems and files, especially those containing sensitive or business critical data.	Line Managers, Data Owners, Product, Project and	All the time

POL00362761

		All Systems must comply with the Access Control Standard.	Programme Managers.	
Personal Data	Due to inadequate training, there is a risk of unintentional misuse of Personal Data, resulting in punitive penalties, reputational damage and a loss of licence to process personal data.	Data Owners must ensure all employees within their areas understand their responsibilities in regard to the protection of personal data.	Data Owners	All the time
		Data Protection must ensure that suitable training is made available to Data Owners and employees.	Data Protection	Annually
Employees	Due to inadequate training, there is a risk of under, or over, retention of information and failure to follow retention schedules, leading to punitive penalties or reputational damage.	All employees must undertake the annual Information Security and Data Protection training. They must also read and understand the Acceptable Use Standard, the Information Classification Standard and this document.	All employees	Annually/ within 3 weeks of starting
		3rd party suppliers must ensure that all employees with access to Post Office data and information undertake Post Office agreed information management training.	3rd party suppliers	Annually/ within 3 weeks of starting
		Ensure annual training contains adequate information on information management.	Data Owners	Annually
		Ensure the Policy Set contains adequate information on Information management.	Data Owners	Annually
Document Management	Failure to keep information evidencing appropriate destruction will increase time spent handling public access requests and will fail to protect Post Office in disputes around information rights regulations (such as Freedom of	Data Owners must ensure that they have defined the storage requirements for the data under their sphere of control, and that this has been documented and agreed. This particularly applies where encryption is required. This is a field within the retention schedule.	Data Owners	Annually/when a change occurs

POL00362761

	Information Act and Data Protection Act).			
Retention Schedules	Lack of communication of required retention schedules may mean that incorrect decisions are made by employees regarding information which could lead to regulatory fines or inability to answer a request to find or correct data.	Data Owners must ensure that correct retention schedules are in place for the systems or product entities within their sphere of control. These are required to be created at project initiation.	Data Owners	Annually/ when a need is identified
		Line managers must ensure that they and all their employees are aware of the retention schedules in place for the data/information they process.	Line Managers	Annually/ when a need is identified
		Line Managers must remain aware of relevant regulatory and legislative requirements for document retention and must regularly review and update retention schedules in line with these as well as functional changes to their area.	Line Managers	Annually/ when a need is identified
Incident Management	Failure to understand the implications of an incident can lead to poor decision making or regulatory sanctions	Employees managing a incident must ensure that the relevant Data Owner is aware of any incidents to their data, and are satisfied with the resolutions.	Data Protection, Cyber Security Team, Physical security.	When an incident occurs
Processes and Procedures	Incorrect processes and procedures can lead to employees incorrectly using data.	Data Owners / Departmental Data Stewards are responsible for ensuring all processes which access the information within their sphere of control are adequate and appropriate.	Data Owners & Departmental Data Stewards	Annually / when a new process or procedure is written

POL00362761

Governance	Lack of governance over documents could lead to incorrect usage of data and thus result in fines or reputational damage to Post Office.	All employees implementing document management practices consistent with this Policy. Preserving documents as required under this Policy.	All employees	All the time
		Properly disposing of information at the end of its retention period.	All employees	All the time
		Monitoring compliance with this Policy.	Respective GE	All the time
		Educating employees in document management practices.	Head of MI, Analytics, Data Strategy, Data Protection and Cyber Team.	Annually
		Maintaining the repository of retention schedules.	Cyber Security	All the time
Legal/ Regulatory Framework	Failure to understand the requirements of any legal or regulatory issues by the Data Owner may lead to Post Office receiving sanctions where documents or entities have not been controlled appropriately	Ensure when creating their Document Retention Schedules all regulatory or legal requirements have been considered.	Data Owners	Annually

During Document/System Disposal

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When

POL00362761

Risks to Information	Incorrectly disposing of information could mean that, through lack of continued controls being implemented for a defunct system/document, Post Office may suffer a data breach.	Data Owners must ensure that they enforce the clauses within a contract at the end of its term.	Data Owners	When a contract closes
		Data Owners must ensure that all users of the entities or documents under their sphere of control understand what actions are to be taken at the end of a retention period.	Data Owners	All the time
		All employees must ensure they understand what needs to be done with a document or system at the end of its retention period.	All Employees	All the time
Document Management	Failure to keep information evidencing appropriate destruction will increase time spent handling public access requests and will fail to protect Post Office in disputes around information rights regulations (such as Freedom of Information Act and Data Protection Act).	The Destruction or transfer of information must be authorised by the Data Owner or Departmental Data Steward and documented so that an audit trail exists.	All employees, Data Owners, Departmental Data Steward	All the time

POL00362761

4. Tools – Retention Schedules

Retention schedules will ensure that retention of information is considered prior to its creation. Some record types can be identified as having definite long-term business or historical value due to the activities they arise from. For others, their value may change over time, or an event (such as an audit or legal action) may require that their scheduled disposal is put on hold. All disposal of information must therefore be approved by the Data Owner before it is actioned and records must be reviewed where this is necessary to make a decision.

Disposal of information at the end of its assigned retention period means either destruction or transfer. Destruction of information must follow Post Office procedures as defined by the Data Owner / Departmental Data Steward in order to prevent a data breach (procedures apply to destruction of hard copy documents, electronic information and hardware). Where documents have been identified as suitable for transfer to The Postal Museum archive Departmental Data Stewards must ensure they comply. This should not be confused with transfer of semi-current or inactive documents to off-site storage facilities. Documents at the end of their retention period must not be transferred to off-site storage facilities unless they are subject to a hold on disposal.

Duplicate documents should be destroyed as soon as possible. Where information has been regularly shared between business units, only the original documents should be retained. Care should be taken that seemingly duplicate documents have not been annotated. Where Post Office shares information with other bodies, Post Office must ensure that they have adequate procedures in place so that the information is managed in accordance with the relevant legislation and regulatory guidance.

4.1. Functional Retention Schedules

Retention schedules set out the groups of documents that Post Office functions will maintain and when these are due for review, transfer to The Postal Museum or secure destruction.

Information on retention schedules will fall into three main categories:

1. Destroy after an agreed period – where the useful life of a group of documents can be easily pre-determined (for example, destroy 3 years after creation; destroy 6 years after the end of the financial year).

2. Automatically select for permanent preservation – where certain groups of documents can be readily defined as worthy of permanent preservation and transferred to The Postal Museum.

3. Review – examine documents to determine whether they should be destroyed, retained for a further period or transferred to The Postal Museum for permanent preservation. Documents which fall under category 1 may need to be reviewed for potential legal hold if they pertain to an active case.

Retention periods and actions are based on informational value, evidential value, legal or regulatory requirements, and historical value.

POL00362761

5. Where to go for help

5.1. Additional Policies

This guideline is one of a set of policies in respect of the use of Information by the Group. The full set of policies can be found at:

https://poluk.sharepoint.com/sites/cybersecurity2/SitePages/Cyber-and-Information-Security-Policy-Set.aspx

5.2. How to raise a concern

Any Post Office employee who suspects dishonest or fraudulent activity has a duty to:

- Discuss the matter fully with their Line Manager; or,
- Report their suspicions by telephoning Grapevine on GRO
- If either or both are not available, staff can contact the Post Office's General Counsel, who can be contacted by email at: GRO or by telephone on: GRO
- Alternatively staff can use the Speak Up service available on GRO
- or via a secure on-line web portal: http://www.intouchfeedback.com/postoffice

Post Office encourages members of the public or people not employed by us who suspect that this policy has not been complied with by a Post Office Employee to write, in confidence, to the **Chief Executive's Office, Finsbury Dials, 20 Finsbury St, London EC2 9AQ** or contact us at https://www.postoffice.co.uk/contact-us

5.3. Who to contact for more information

If you need further information about this policy or wish to report an issue in relation to this policy, please contact Cyber Security Team via GRO

POL00362761

6. Control

6.1. Policy Version

Date	Version	Updated by	Change Details
26/02/2018	0.1	IPA & CoSec	First draft Version
04/03/2018	0.2	IPA & Head of MI, Analytics and Data Strategy	Edits following peer review.
07/03/2018	1.0	General Counsel	First Final Version
21/03/2018	1.1	IPA	Updated with minor comments after RCC
3/07/2020	1.2	Cyber Security	Updated to reflect the current policy structure
13/07/2020	1.3	RCC	Approved in RCC

6.2. Policy Approval

Group Oversight Committee:	Risk and Compliance Committee (RCC)
Sign-off Authority:	Risk and Compliance Committee (RCC)
Policy Sponsor:	Chief Information Officer
Policy Owner:	Chief Information Security Officer
Policy Author:	Ehtsham Ali
Approved by:	Post Office Management Services Limited RCC Post Office Ltd RCC
Approved:	13/07/2020
Next review:	13/07/2020