Group policy

Data Protection Policy

Version 1.0 | Public | January 2025

POST OFFICE

Contents

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 the collection, use, retention, transfer, disclosure, and destruction of personal data contrary to data protection legislation.

1.2 Purpose

The purpose of this policy is to provide a consistent, coherent, and proportionate approach to data protection and set out the minimum operating standards to manage associated risks throughout the group.

To achieve this, the Post Office will:

I. Maintain an effective governance and assurance environment in respect of data protection.

II. Comply with all applicable legal and regulatory requirements relating to data protection.

III. Cultivate a setting that minimises personal data incidents and breaches.

The Policy 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 and in the context of applicable legislation and regulations (see Appendix 2). Compliance with these policies supports the Post Office in meeting its business objectives and to balance the needs of our shareholder, 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 legal entities, franchise partners and subsidiaries

[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.

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

In order to manage the legal and regulatory risks associated with data protection and establish processes for the identification and management of them, the governance arrangements included in this Policy are based upon the following core principles:

a. Post Office promotes ethical and professional standards to ensure that the rights of individuals are at the forefront of decision making;

b. Post Office are committed to promote Privacy by Design principles into all processes and systems to ensure protection of personal data;

c. Every member of staff is responsible for understanding and managing data protection risks;

d. Clear accountabilities, commensurate with the tasks, are delegated to people who have the right level of skill, competency and experience;

e. Post Office are committed to manage personal data fairly and effectively. To achieve this, the process for identifying, disclosing and managing personal data must be transparent;

f. Foster an environment where personal data incidents and breaches are mitigated through robust incident and breach management.

g. Post Office are committed that any third parties handling personal data comply with the same data protection standards.

h. A commitment to providing appropriate training and awareness of data protection.

Data Protection Principles

Post Office follows the data protection principles, as laid out in legislation, to govern the processing of personal data, where Post Office is controller:

1. **Lawfulness, Fairness and Transparency**

Post Office must process personal data lawfully, fairly and in a transparent manner. Post Office must provide a privacy notice which informs relevant data subjects about how and why Post Office processes their personal data and must ensure that the description is thorough and clear.

2. **Purpose Limitation**

Post Office must only use personal data for the purpose that it was originally collected and limit any further processing of that personal data in accordance with the purposes notified to the data subject and as permitted under data protection legislation.

3. Data Minimisation

The personal data that Post Office processes must be adequate, relevant, and limited to what is necessary in relation to the purpose(s) for which they are processed. This means Post Office must not process any personal data beyond what is strictly required.

4. Accuracy

The personal data processed by Post Office must be accurate and kept up to date. Post Office must ensure that processes for identifying and addressing out-of-date, incorrect and redundant personal data are introduced and maintained.

5. Storage Limitation

Personal data shall be kept no longer than necessary, and in accordance with the original purpose for which the personal data was processed, through the implementation of an effective process of document and records management. Post Office shall operate an effective records retention schedule.

Personal data should be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Post Office must, wherever possible, introduce mechanisms and procedures into their systems and processes that limits or prevents identification of the data subject (e.g. anonymisation, pseudonymisation, etc).

6. Integrity & Confidentiality

Post Office must process personal data in a manner that ensures appropriate security including protection against unauthorised or unlawful processing, and accidental loss, destruction or damage. Post Office must use appropriate technical and organisational measures to ensure the integrity and confidentiality of personal data is always maintained.

7. Accountability

Post Office must demonstrate that these data protection principles are met for all personal data processing for which it is responsible as controller. Post Office shall maintain records of processing activities (RoPA) which identifies where personal data forms part of business processing activities and ensure these are regularly reviewed. RoPAs are maintained whether Post Office is controller or processor.

It shall be the responsibility of the Strategic Executive Group (SEG) to ensure that all processes for which they are responsible, are conducted in a manner which can be subject to either internal audit and/or external regulatory scrutiny, and can demonstrate their compliance with this policy, its corresponding standards and guidance and legal requirements.

Data Subject Rights

Where Post Office is a controller, individuals have the following rights under legislation;

- Right of access (to personal data). The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning them are being processed, and, where that is the case, access to the personal data;
- Right to rectification. The data subject shall have the right to obtain from the Post Office without undue delay the rectification of inaccurate personal data concerning him or her;
- Right to be informed. The data subject has the right to know, amongst other things, what personal data is processed about them and under which lawful basis. This is usually communicated through the provision of a privacy notice;
- Right to erasure. The data subject shall have the right to obtain from the Post Office the erasure of personal data concerning them without undue delay and the controller shall have the obligation to erase personal data without undue delay under certain circumstances;
- Right to restriction of processing. The data subject shall have the right to obtain from the controller restriction of processing under certain circumstances, for example temporarily moving personal data to another processing system.
- Right to object to processing (including automated decision-making and profiling). The data subject shall have the right to object, on grounds relating to their particular situation, at any time to processing of personal data concerning him or her under certain circumstances; and
- Right to data portability. In certain circumstances the data subject shall have the right to receive the personal data concerning them, which they have provided to Post Office, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller

Special Category Data Processing

This policy responds to the requirement for an appropriate policy document in context of the Data Protection Act, schedule 1, part 4. Post Office processes certain types of sensitive personal data, known as special category personal data, for purposes including but not limited to;

- employment purposes;
- the provision of Travel Insurance and in the management of policies;
- processing legal claims including under any relevant compensation schemes.

This processing is described in the OneTrust system, maintained by the data protection team. It records the relevant lawful basis that is being relied upon in order to process the personal data, where Post Office is controller.

Post Office may also process, under contract, special category personal data as a processor, as instructed by controllers who are clients of Post Office.

Criminal Offence Data Processing

This policy responds to the requirement for an appropriate policy document in context of the Data Protection Act, schedule 1, part 4. Post Office processes criminal offence data for the following purposes:

- vetting checks for employment;
- onboarding of postmasters and their assistants;
- Fit & Proper declarations for postmasters and other responsible persons; and
- in reponse to legal claims.

This processing is described in the OneTrust system, the privacy management platform maintained by the data protection team. It records the relevant lawful basis that is being relied upon in order to process the personal data, where Post Office is controller.

Special category and criminal offence data will be managed in accordance with Post Office's record retention schedules.

1.5 Policy Framework

The Data Protection 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 (RCC), 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 Where to go for help

2.1 Reporting Non-Compliance

Where non-compliance is identified, the matter must be referred to the Policy Owner, which is the Head of Data Protection and Information Rights. 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.

Where external non-compliance is identified, individuals may wish to reach out to the Information Commissioner's Office (ICO) through a number of channels found at:

https://ico.org.uk/make-a-complaint/

2.2 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

3 Document control

3.1 Document control record

Summary

Version	Document review period	Policy – effective date	Policy location
V1.0	Annual	January 2025	https://corporate.postoffice.co.uk/en/governance/post-office-policies/post-office-policies/

3.2 Policy Approval

Committee	Date approved
POL R&CC	**10/03/25**
POL ARC	**25/03/25**
POMS ARC	**29/07/25**

Next policy annual review date: 01/01/2026

Appendices

Definitions

Controller - means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data Protection Legislation - means the Data Protection Act 2018, UK GDPR and all relevant privacy legislation.

Personal Data - in the context for Post Office, this refers to any information that relates to an individual and can be used to identify them. Including but not limited to; an individual's name, telephone number and CCTV images of individuals but also data that initially is not considered to be personal data such as a car registration number when provided against other identifiable indicators.

Processor - means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller.

Records of Processing Activities (RoPA) - means records of processing activities, as described in Article 30 of the UK GDPR.

Special Category Personal Data - personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Criminal Offence Data – this covers information about offenders or suspected offenders in the context of criminal activity, allegations, investigations and proceedings.

Strategic Executive Group (SEG) - the Strategic Executive Group consists of all the senior leaders for each business directorate.

Process Owner – means the member of staff who is responsible for the processing activity.

Applicable regulation and legislation

The Post Office Group seeks to comply with all relevant legal and regulatory requirements including, but not limited to, the following (as amended or supplemented from time to time):

- Data Protection Act 2018 (DPA)
- UK General Data Protection Regulation 2021 (UK GDPR)
- Privacy & Electronic Communications (EC Directive) Regulations 2003 (PECR)
- Human Rights Act 1998
- The Protection of Freedoms Act 2012

The Information Commissioner's Office (ICO) and the Financial Conduct Authority (FCA) issue codes of practice, guidance, and self-assessment tools under the relevant legislation which assist Post Office in meeting their legal and regulatory obligations.

For further information regarding the DPA, UK GDPR and PECR, please visit the UK data protection regulator, the Information Commissioner's Office (ICO) on the following link: https://ico.org.uk/.

Governance Responsibilities

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

The Policy Owner is the Head of Data Protection and Information Rights Manager who is responsible for ensuring that the content is up to date and is capable of being executed. The Head of Data Protection and Information Rights Manager is responsible for providing appropriate and timely reporting to the Risk and Compliance Committee and the Audit, Risk and Compliance 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.