

Group policy

Data Protection Policy

Version 1.1 | Public | May 2026



Contents

1	Overview	3
1.1	Introduction	3
1.2	Purpose	3
1.3	Who Must Comply	3
1.4	Core Principles	4
1.5	Policy Framework	7
2	Where to go for help	8
2.1	Ethical Decision-Making Model	8
2.2	Reporting Non-Compliance	8
2.3	Reporting a Concern – How to ‘Speak Up’	8
3	Document control	9
3.1	Document control record	9
3.2	Policy Approval	9
4	Appendices	10
	Appendix 1 – Definitions	10
	Appendix 2 - Applicable regulation and legislation	10
	Appendix 3 - Governance Responsibilities	11

1 Overview

1.1 Introduction

The Chief Operations Officer has overall accountability to the Post Office Group¹ Boards for the design and implementation of effective 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 Data Protection Policy (the “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 an organisational environment that minimises the impact and occurrence of personal data incidents and breaches.

The Policy operates alongside a number of other policies that together form a clear governance and internal control framework for managing risk across Post Office and ensuring compliance with applicable legislation and regulations (see Appendix 2). Compliance with these policies supports the Post Office in meeting its business objectives and balancing the needs of our shareholder, and other stakeholders.

1.3 Who Must Comply

Compliance with this Policy is mandatory for:

- All employees² 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

Post Office adopts a principles-based approach to data protection compliance, meaning we focus on the data protection principles set out in relevant legislation and core organisational values, rather than relying solely on prescriptive or checklist-style rules. This approach provides a clear and consistent foundation for making decisions about how personal data is collected, used, shared, and protected, and supports a culture where everyone understands their role in managing personal data.

Our core organisational principles are:

- a. Post Office promotes ethical and professional standards, ensuring that the rights of individuals are central to decision-making.
- b. Post Office is committed to embedding Privacy by Design into all processes and systems to support the protection of personal data.
- c. Every member of staff is responsible for complying with data protection obligations, including the identification and management of data protection risks.
- d. Clear accountabilities are assigned to individuals with the appropriate skills, competence, and experience to discharge them effectively.
- e. Post Office is committed to managing personal data fairly and effectively, supported by transparent processes for identifying, disclosing, and managing personal data.
- f. Post Office fosters an environment where personal data incidents and breaches are prevented and mitigated through robust incident and breach management.
- g. Post Office ensures that any third parties handling personal data meet equivalent data protection standards.
- h. Post Office is committed to providing appropriate data protection training and awareness to ensure staff understand their responsibilities.

Data Protection Principles

Post Office follows the data protection principles set out in relevant legislation to guide the processing of personal data where Post Office acts as a data controller:

1. Lawfulness, Fairness and Transparency

Post Office processes personal data lawfully, fairly and in a transparent manner. Post Office provides privacy notices which inform relevant individuals 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 only uses 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 individual 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 will not process any personal data beyond what is required.

4. Accuracy

The personal data processed by Post Office must be accurate and kept up to date. Post Office ensures 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 retained for as long as necessary for the purposes for which it was originally collected and processed. Post Office applies effective records-management and retention schedules to ensure data is held only for appropriate periods.

Where possible and appropriate, Post Office implements measures such as anonymisation or pseudonymisation to reduce or prevent the identification of individuals during processing.

6. Integrity & Confidentiality

Post Office processes personal data in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage.

To support this, Post Office implements appropriate technical and organisational measures designed to maintain the integrity and confidentiality of personal data at all times.

7. Accountability

Post Office is accountable for demonstrating that the data protection principles are met for all personal data processing where it acts as controller. Post Office maintains a Record of Processing Activities (RoPA) that identifies where personal data forms part of business processes, and ensures these records are reviewed regularly.

Post Office Executive (Exec) is responsible for ensuring that the processes within their remit can withstand internal audit and external regulatory scrutiny, and for demonstrating compliance with this Policy, the associated standards and guidance, and all applicable legal requirements.

Legislative and Regulatory Framework

This Data Protection Policy is based on the UK's data protection and privacy legislative framework, which governs the lawful, fair and transparent processing of personal data and provides individuals with enforceable rights over their personal data.

Post Office processes personal data in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, which together set out the core principles for processing, the lawful bases on which personal data may be used and the rights of individuals. These laws also establish accountability obligations requiring organisations to demonstrate compliance through appropriate governance, controls and safeguards.

The Data (Use and Access) Act 2025 amends and supplements the UK GDPR, the Data Protection Act 2018 and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR), updating certain aspects of personal data use while clarifying protections for individuals. Post Office applies the requirements of the DUAA as part of its overall approach to data protection compliance, alongside other relevant legislation, including human rights and surveillance-related statutes where applicable.

This Policy provides the overarching framework for compliance with these legal requirements. Further detail on how specific obligations are implemented in practice is set out in supporting procedures, standards, notices and guidance.

Individual Rights

Where Post Office is processing personal data as a controller, individuals have the following rights under legislation;

- Right of access (to personal data): Individuals shall have the right to obtain from Post Office confirmation as to whether or not personal data concerning them is being processed, and, where that is the case, access to the personal data;
- Right to be informed: Individuals have the right to know what personal data is processed about them and under which lawful basis. This is usually communicated through a privacy notice;
- Right to complain: Individuals have the right to complain to Post Office if they think that the processing of their personal data has not been managed responsibly, in line with Post Office's legal obligations as a controller. Post Office provides a variety of channels for individuals to get in touch and will respond to complaints without undue delay.
- Right to rectification: Individuals shall have the right, without undue delay, for Post Office to correct any inaccurate or incomplete personal data that is processed relating to them;
- Right to erasure: Individuals have the right to request Post Office erases the personal data it processes concerning them, which Post Office is obliged to comply without undue delay under certain circumstances;
- Right to restriction of processing: Individuals have the right to request Post Office restricts processing of their personal data under certain circumstances. This could include, for example, temporarily moving their data to a separate system.
- Right to object to processing (including automated decision-making and profiling): Individuals have the right to object, on grounds relating to their particular situation, where decisions are made using their personal data without people being involved; and
- Right to data portability: Individuals have the right to receive an accessible and machine readable copy of their personal data, where they have provided it to Post Office, and have their data transferred to another controller

Special Category Data Processing

This Policy forms part of the organisational measures used to meet the requirement for an appropriate policy document under Schedule 1, Part 4 of the Data Protection Act 2018. Activity specific details, including the relevant conditions relied upon, are documented within the RoPA.

Post Office processes certain types of sensitive personal data, known as special category data, for purposes including, but not limited to;

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

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 forms part of the organisational measures used to meet the requirement for an appropriate policy document under Schedule 1, Part 4 of the Data Protection Act 2018. Activity specific details, including the relevant conditions relied upon, are documented within the RoPA.

Post Office processes criminal offence data for the following purposes:

- Employment-related vetting checks;
- Onboarding of postmasters and their assistants;
- Fit & Proper declarations for postmasters and other responsible persons;
- Responding to legal claims; and
- Supporting law enforcement and loss-prevention activities.

Special category data and criminal offence data are managed in accordance with Post Office's records-management and retention schedules.

1.5 Policy Framework

This Policy is reviewed and updated at least annually, and more frequently where required, to ensure it remains relevant, aligns with legislative and regulatory developments, and reflects lessons learned from both internal and external events.

As a Group Key Policy, it is subject to annual review and endorsement by the Risk and Compliance Committee (RCC), the Audit, Risk and Compliance Committee (ARC), and, where appropriate, the Board. Once approved, the Policy is adopted by Post Office Limited and its wholly-owned subsidiaries³.

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

2 Where to go for help

2.1 Ethical Decision-Making Model

Post Office policies and guidelines can support in de-risking our decisions, however they cannot cover every eventuality. All users of this Policy should have regard to the Ethical Decision-Making Model and report decisions that don't follow this model, as instructed below.

A link can be found here [POL Ethical Decision Making Model](#)

2.2 Reporting Non-Compliance

Where instances of non-compliance with this Policy are identified, they should be reported to the Policy Owner, via data.protection@postoffice.co.uk. Any investigations, where required, will be undertaken in accordance with the Investigations Policy. Where non-compliance arises from wilful disregard or negligence, this may be treated as a disciplinary matter.

Individuals also have the right to raise concerns externally with the Information Commissioner's Office (ICO). Information on how to contact the ICO is available at:

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

2.3 Reporting a Concern – How to 'Speak Up'

Post Office strives to foster an environment where everyone feels able to speak up. We encourage anyone to raise concerns about suspected wrongdoing, illegal activity, unethical behaviour, or any matter that may compromise the integrity of our operations.

Information and contact details for the confidential Speak Up service can be found below:

- 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/
V1.1	Annual	April 2026	https://corporate.postoffice.co.uk/en/governance/post-office-policies/post-office-policies/

3.2 Policy Approval

Committee	Date approved
POL RCC	28/04/2026
POL ARC	19/05/2026
POMS ARC	19/05/2026

Next Policy annual review date: 01/04/2027

4 Appendices

Appendix 1 – Definitions

Data 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, DUAA and all relevant privacy legislation.

Personal Data – in the context of Post Office, this refers to any information that can identify an individual, either on its own or combined with other information. This can include but is not limited to; an individual's name, telephone number and CCTV images of individuals but also information that may not initially be considered to be personal data such as a tracking barcodes and IP addresses.

Data 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 a record of processing activities, as described in Article 30 of the UK GDPR.

Accountability Framework – a framework tracker published by the Information Commissioner's Office (ICO) as part of their data protection audit framework, that helps organisations demonstrate compliance with UK data protection law. It sets out the ICO's expectations for how organisations should embed accountability by implementing appropriate and effective technical and organisational measures.

Special Category Personal Data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying an individual and data concerning an individual's health, 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.

Executive (Exec) – the Executive consists of all the senior leaders for each business directorate.

Appendix 2 - 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)
- Data Use and Access Act 2025 (DUAA)
- 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 its 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/>.

Appendix 3 - Governance Responsibilities

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

The Policy Owner is the Resilience Director, who is responsible for ensuring that the content is up to date and is capable of being executed. The Policy Owner 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.

Post Office Limited and Post Office Management Services Limited are registered in England and Wales. Registered numbers 2154540 and 08459718, respectively. Registered Office: 100 Wood Street, London, EC2V 7ER

Post Office Management Services Limited is authorised and regulated by the Financial Conduct Authority (FCA), FRN 630318. Its Information Commissioners Office registration number is ZA090585.

Post Office Limited is authorised and regulated by Her Majesty's Revenue and Customs (HMRC), REF 12137104. Its Information Commissioners Office registration number is Z4866081.

