Co-operatives UK Data Protection Policy

Policy Owner:	Data Protection Lead
Version:	V.3 (original version May 2018)
Reviewed by:	Data Protection Lead
Last Reviewed:	January 2026
Next Review Due:	February 2029
Approved by:	Approved by LT on: 24 February 2026
Key Messages:	• Outlines Co-operatives UK's approach to compliance with data protection requirements
Associated documents	• To be read alongside Record of Processing Activities, Privacy Notices, Special Category Data Policy, CCTV Policy and Data Retention Policy

1. Policy Statement

Every day our business will receive, use and store personal information about our members, clients, suppliers, beneficiaries and staff. It is important that this information is handled lawfully and appropriately in line with the requirements of the Data Protection Act 2018 and the UK General Data Protection Regulation (collectively referred to as the 'Data Protection Requirements').

We take our data protection duties seriously, because we respect the trust that is being placed in us to use personal information appropriately and responsibly.

2. About This Policy

This policy, and any other documents referred to in it, sets out the basis on which we will process any personal data regardless of the media on which that data is stored or who it relates to. This policy does not form part of any contracts and may be amended at any time.

Our data protection lead, Zena King - Senior Governance Advisor, is responsible for ensuring compliance with the Data Protection Requirements and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to Zena King - Senior Governance Advisor.

This Data Protection Policy applies to all Co-operatives UK staff; they must read, understand and comply with it when processing personal data on our behalf and attend training on its requirements. Data protection is the responsibility of everyone within the organisation and this Policy sets out our expectations when personal data is being processed. Members of staff may have specific responsibilities to ensure compliance with data protection requirements as part of their role, for example capturing consent to process personal data, reporting data breaches or conducting data protection impact assessments - supporting guidance is available in our related policies, procedures, templates and privacy notices.

We will keep accurate records of all our personal data processing activities, including data sharing agreements and records of consents to process personal data.

3. What is Personal Data?

Personal data means data (whether stored electronically or paper based) relating to a living individual who can be identified directly or indirectly from that data (or from that data and other information in our possession). Data relating to an organisation is not personal data.

Processing is any activity that involves use of personal data. It includes obtaining, recording or holding the data, organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

Special category data (sometimes referred to as 'sensitive personal data') includes data about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic, biometric, physical or mental health condition, sexual orientation or sexual life. It can also include data about criminal offences or convictions.

4. Data Protection Principles

Anyone processing personal data, must ensure that it is:

- Processed fairly, lawfully and in a transparent manner.
- Collected for specified, explicit and legitimate purposes and any further processing is for a compatible purpose.
- Adequate, relevant and limited to what is necessary for the intended purposes.
- Accurate, and where necessary, kept up to date.
- Kept in a form which permits identification for no longer than necessary for the intended purposes.
- Processed in line with the individual's rights and in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- Not transferred to another country without appropriate safeguards in place (transfer limitation); and
- Made available to data subjects if they wish to exercise certain rights in relation to their own data.

As we have fewer than 250 employees, we may only maintain records of processing activities that are not occasional; could result in a risk to the rights and freedoms of individuals; or involve the processing of special category data.

Where a new activity is proposed which is likely to involve large-scale processing of personal data or the processing of special category data which may result in a risk to the rights and freedoms of individuals, a data protection impact assessment will be completed before the activity commences.

5. Fair and Lawful Processing

The UK GDPR and Data Protection Requirements are not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the individual. In accordance with Data Protection Requirements, we will only process personal data where it is required for a lawful purpose. The lawful purposes include (amongst others):

- Where the individual has given their explicit consent by opting into their personal data being used for that specific purpose. Consent to data processing can be withdrawn by the data subject at any time.
- The processing is necessary for performing a contract with the individual.
- For compliance with a legal obligation.
- To pursue our organisation's legitimate interests where they are not overridden because the processing prejudices the interests or fundamental rights and freedoms of the individual.

Where the data subject's consent is required to process their personal data, employees must retain evidence that consent has been properly obtained so that Co-operatives UK can demonstrate compliance with Data Protection Requirements.

Co-operatives UK does not use Automated Processing (including profiling) and Automated Decision Making.

6. Processing for Limited Purposes

In the course of our business, we may collect and process the personal data set out in our Record of Processing Activities (available for staff in our Policies folder and for others on request). The majority of the data we process will be received directly from data subjects (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) but we also sometimes receive from other sources (including, for example, location data, business partners, sub-contractors in technical, payment and delivery services, credit reference agencies and others).

We will only process personal data for the specific purposes set out in our Record of Processing Activities (available for staff in our Policies folder and for others on request) or for any other purposes specifically permitted by the Data Protection Requirements. We will not use personal data for new, different or incompatible purposes from that documented in our Record of Processing Activities and Privacy Notices. If an employee wishes to use personal data for a new or different purpose from that for which it was obtained, they must first contact the Data Protection Lead for advice.

7. Transparency (notifying data subjects)

Co-operatives UK will ensure that appropriate Privacy Notices are accessible by data subjects to inform them concisely and transparently about how we intend to use their personal data and details of our Data Protection Lead.

When personal data is collected indirectly (for example, from a third party or publicly available source), we will provide the data subject with information required by the UK GDPR as soon as possible after collecting or receiving the data. We must also check that the personal data was collected by the third party in accordance with the UK GDPR and on a basis which contemplates our proposed processing.

8. Adequate, Relevant and Non-excessive Processing

We will only collect personal data to the extent that it is required for the specific purpose notified to the data subject. Members of staff will only collect and process personal data whilst performing duties associated with their role. It is their individual responsibility to ensure that they do not collect excessive or irrelevant data and that when it is no longer needed personal data is deleted or anonymised in accordance with our Data Retention Policy.

9. Accurate Data

We will endeavour to ensure that personal data we hold is accurate and kept up to date. We will check the accuracy of any personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

10. Timely Processing

We will not keep personal data longer than is necessary for the purpose or purposes for which it was collected. We will take all reasonable steps to anonymise, destroy or erase from our systems, all data which is no longer required. Please refer to our Data Retention Policy for a comprehensive guide to the storage, use and deletion of data after the purpose for processing has ended.

11. Processing in line with Data Subject's Rights

We will process all personal data in line with data subjects' rights, in particular their right to:

- Confirmation as to whether or not personal data concerning them is being processed.
- Request access to any data held about them by a data controller
- Request rectification, erasure or restriction on processing of their personal data.
- Lodge a complaint with a supervisory authority.
- Data portability.
- Object to processing including for direct marketing.
- Not be subject to automated decision-making including profiling in certain circumstances.

Our staff must verify the identity of an individual requesting data under any of the rights listed above (we will not disclose personal data under any circumstances without proper authorisation).

12. Data Security

We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental or unlawful destruction, damage, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed.

We will put in place procedures and technologies to maintain the security of all personal data from the point of the determination of the means for processing and point of data collection to the point of destruction. Personal data will only be transferred to a data processor if they agree to comply with those procedures and policies, or if they put in place adequate measures.

We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

- **Confidentiality** means that only people who are authorised to use the data can access it.
- **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.
- **Availability** means that authorised users should be able to access the data if they need it for authorised purposes, such as auditing. Personal data should therefore be stored on Co-operatives UK's approved data systems and not on individual devices.

Employees must comply with, and not attempt to circumvent, the administrative, physical and technical safeguards we implement and maintain to protect personal data.
Security procedures include:

- **Entry controls.** Any stranger seen in entry-controlled areas of our office should be reported to the facilities manager.
- **Secure lockable storage.** Lockers should be kept locked if they hold confidential information of any kind. When members of staff are working from home they will ensure no one else can access their equipment or personal data they hold for work purposes.
- **Data minimisation.** Alongside ensuring we only gather and hold necessary personal data, this also includes storing data within our approved data storage system and only printing data if it is absolutely necessary.
- **Pseudonymisation and encryption of data.** Where appropriate to minimize our use of personal data and to facilitate safe storage and transfer when necessary. The Digital Team are able to support these processes when needed.
- **Methods of disposal.** Paper documents should be disposed of in confidential waste bins. Digital storage devices should be physically destroyed by the Digital Team when they are no longer required.
- **Equipment.** Staff must ensure that individual monitors do not show confidential information to passers-by and that devices are password protected when left unattended. All devices should be encrypted and portable devices, such as laptops and tablets, should be securely stored when left unattended. Any lost or stolen equipment must be reported immediately to the Digital Team to ensure,

where possible, its contents are wiped via remote access. More details are outlined in our IT Use Policy.

13. Transferring Personal Data Outside the UK

We may transfer any personal data we hold to a country outside the UK or to an international organisation, provided that one of the following conditions applies:

- The country to which the personal data is transferred ensures an adequate level of protection for the data subjects' rights and freedoms.
- The data subject has given consent.
- The transfer is necessary for one of the reasons set out in Data Protection Requirements, including the performance of a contract between us and the data subject, or to protect the vital interests of the data subject.
- The transfer is legally required on important public interest grounds or for the establishment, exercise or to defend legal claims.
- The transfer is authorised by the relevant data protection authority where we have adduced adequate safeguards with respect to the protection of the data subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights.

Subject to the requirements above, personal data we hold may also be processed by staff operating outside the UK who work for us or for one of our suppliers. Those staff may be engaged in, among other things, the fulfilment of contracts with the data subject, the processing of payment details and the provision of support services.

14. Sharing Personal Data

Co-operatives UK will not ordinarily share personal data, we will only share information outside the organisation where adequate safeguards have been put in place in protect that data.

A member of staff will only share personal data that we hold with another member of staff, agent or representative of our organisation if the recipient has a job-related need to know the information. We will only share personal data that we hold with third parties if:

- they have a need to know the information for the purposes of providing contracted services;
- sharing the personal data complies with our Privacy Notice and, if required, the data subject's consent has been obtained;
- the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
- the transfer complies with any requirements regarding transfer outside of the UK; and
- there is a data sharing agreement in place with the recipient of the personal data.

15. Third party contracts

Contracts with third parties should stipulate the role of each party and the limits on the use of the data. The contracts should state which party is the data controller and who is the data processor.

Broad definitions of these roles are:

- A **data controller** is the organisation who determines how and why the data should be collected and processed.
- A **data processor** will act on the orders of the controller and at no point will use judgement or decision making with regards the data.

It is possible that a single organisation can be both a data processor and a data controller in relation to different processing activities (it cannot be both a controller and a processor for the same processing activity).

The distinction is not always easy to make but the ICO provides useful guidance 'data controllers and data processors'.

16. Reporting Personal Data Breaches

All personal data breaches must be logged, and certain personal data breaches must be reported to the Information Commissioner and the data subject. We procedures in place to deal with any suspected personal data breaches and we will notify the data subject and regulators where we are required to.

In the event of a suspected breach of personal data, members of staff are required to contact the Data Protection Lead (the Society Secretary or their Line Manager if the Data Protection Lead is not available). They must not attempt to investigate the breach themselves and must preserve all evidence related to the suspected breach.

17. Direct marketing

Data Protection Requirements and privacy laws also govern some of our activity to market our services and events. The majority of our marketing is via email to individuals who have a formal relationship with an organisation that is a member of Co-operatives UK (they are either employees, members or directors of that organisation). Such individuals can be defined as 'corporate subscribers' and we have documented our legitimate interest in informing them of our services and events. As a result, we do not require their consent to receive marketing information in order to comply with data protection requirements and privacy laws.

We will always provide data subjects with the opportunity to stop receiving marketing information from us and when requested, we will ensure their details are suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

Details of the lawful basis for any marketing to individuals who do not meet the definition of 'corporate subscribers' will be available in our privacy notice(s).

18. Data Subject Access Requests

Where a data subject requests confirmation as to whether or not we are processing personal data concerning them or requests access to any data held about them, they will be asked to submit this as a formal 'Data Subject Access Request'. A member of staff receiving such a request (or any request that they believe may be a request for access to personal data) should forward it to the Data Protection Lead immediately. Any member of staff may be required to assist in responding to a Data Subject Access Request to enable full compliance with Data Protection Requirements.

When receiving telephone enquiries, we will only disclose personal data we hold on our systems if we are sure that the caller is entitled to the information and we have been able to verify the caller's identity.

Where a request is made electronically, data will be provided electronically where possible. It may not always be possible to provide data in hard copy format.

19. Privacy by Design and Data Protection Impact Assessments (DPIA)

Data Protection Requirements include implementing a 'Privacy by Design' approach to our work and data processing systems ensuring that personal data is protected in a way that is appropriate for the size and scale of our organisation and the nature of our activities.

Members of staff are required to conduct DPIAs using the template provided and discuss their findings with the Data Protection Lead when implementing major system changes, projects or new activities which involved significant processing of personal data including:

- Use of new technologies (programs, systems or processes, including the use of AI), or changing technologies (programs, systems or processes).
- Automated Processing including profiling and ADM.
- Large-scale Processing of Special Categories of Personal Data or Criminal Convictions Data.
- Large-scale, systematic monitoring of a publicly accessible area.

20. Staff training

We will ensure that our staff team completes appropriate training to enable them to understand and comply with the Data Protection Requirements relevant to their role. Members of staff will be provided with a full induction on Data Protection Requirements, access to support and guidance from the Data Protection Lead and to independent expert advice if they deem this necessary. Periodic training will be provided for all staff including following any significant changes to Data Protection Requirements or Co-operatives UK's activities; such training will be mandatory.

We will also regularly test our systems and processes to assess compliance and require members of staff to regularly review their team's systems and processes to ensure:

- they comply with our data protection policies; and
- to check that adequate governance controls and resources are in place to ensure proper use, protection and erasure of personal data.

21. Policy Owner and Review

The current owner of this policy is Zena King - Senior Governance Advisor who will from time to time review the implementation of the Data Protection Policy in respect of its suitability, adequacy and effectiveness and make improvements where appropriate. The Policy will then be submitted to the Leadership Team for approval.

CO-OPERATIVES UK