CDS Co-operatives

DATA PROTECTION POLICY

Date Approved	22 September 2025
Responsible officer	Christina Friedenthal, Corporate Services Director
Review date	September 2028

CONTENTS

1.0 Introduction

1.1 The Co-operative Development Society Ltd (CDS) is committed to ensuring the secure and safe management of data held by CDS in relation to customers, staff and other individuals. CDS staff members have a responsibility to ensure compliance with the terms of this policy, and to manage individuals' data in accordance with this policy and any associated procedures.

1.2 CDS needs to gather and use certain information about individuals. These can include customers (tenants and leaseholders of CDS, tenants and leaseholders of client organisations, applicants for accommodation), employees and other individuals that CDS has a relationship with.

1.3 CDS manages a significant amount of data from a variety of sources. This includes Personal Data and Special Categories of Personal Data (previously referred to as Sensitive Personal Data).

1.4 This policy sets out CDS's duties in processing that data and the purpose of this policy is to set out the principles for the management of such data in compliance with the Data Protection Act 2018 which implements in UK law the requirements of the UK General Data Protection Regulations (UK GDPR) effective 1st January 2021.

1.5 The GDPR sets out six principles for the lawful processing of personal data:

i. Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');

ii. Personal data shall only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation');

iii. Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

iv. Personal data shall be accurate and, where necessary kept up to date ('accuracy');

v. Personal data shall 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 are processed ('storage limitation');

vi. Personal data shall be processed 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 and organisational measures ('integrity and confidentiality');

1.6 CDS shall be responsible for, and be able to demonstrate compliance with, the above principles.

1.7 CDS has appointed the Corporate Services Director (CSD) as the Data Protection Lead. The CSD will take charge of the day-to-day management of data protection.

1.8 This policy applies to all employees, board members and others who may be involved in the collection and processing of personal information on behalf of CDS and extends to data whether it is held on paper or by electronic means.

1.9 As a minimum, this policy applies when CDS is processing personal data in respect of customers of any organisation that has a management agreement with CDS for the provision of services. However, CDS will also meet any additional obligations placed on it by the client organisation in their role as a data controller in respect of personal data.

2 Statement of Commitment

2.1 CDS is committed to maintaining high standards of security and confidentiality for information in our custody and control. Protecting this information is critical to the successful operation of CDS. CDS will treat all information in its care and control with the same degree of security and confidentiality.

2.2 CDS undertakes to inform residents, contractors, employees and board members on how it uses information and the purposes for which information is processed.

3 Legislation

3.1 It is a legal requirement that CDS processes data correctly; CDS must collect, handle and store personal information in accordance with the relevant legislation;

3.2 The relevant legislation in relation to the processing of data is:

- The General Data Protection Regulation (EU) 2016/679 “GDPR”;
- UK General Data Protection Regulations (UK GDPR) effective 1st January 2021
- The Privacy & Electronic Communications (EC Directive) Regulations 2003
- The Data (Use and Access) Act 2025 (DUAA)

4 Data

4.1 CDS holds a variety of data relating to individuals, including customers and employees (data subjects), which is known as Personal Data. The Personal Data held and processed by CDS is detailed in our Privacy Notice (Customers), our Privacy Notice (Employees) and our Privacy Notice (CLH Hub for London) which are attached as appendix 1 to this policy.

4.2 "Personal Data" is that from which a living individual can be identified either by that data along or in conjunction with other data held by CDS.

4.3 also hold Personal Data that is sensitive in nature (i.e. relates to or reveals a data subject's racial or ethnic origin, religious beliefs, political opinions, health matters or sexual orientation). This is "Special Category Personal Data".

5 Processing of Personal Data

5.1 The legislation sets out the basis on which Personal Data may be processed by a data controller. For CDS these are:

i. Processing with the consent of the data subject;

ii. Processing is necessary for the performance of a contract between the CDS and the data subject or for entering into a contract with the data subject;

iii. Processing is necessary for CDS's compliance with a legal obligation;

iv. Processing is necessary to protect the vital interests of the data subject or another person;

v. Processing is necessary for the performance of a task carried out in the public interest or in the exercise of CDS's official authority; or

vi. Processing is necessary for the purposes of legitimate interests.

5.2 CDS will maintain a **data map** that schedules the categories of individuals and the categories of personal data that it may collect in respect of those individuals. For each category the map will detail:

- Categories of external recipients with whom that data may be shared;
- The retention period for the detail;
- The lawful basis for processing (as detailed in section 5.1);
- The source of the personal data;
- For Special Category Data the additional lawful basis for processing.

5.3 The data map will be kept regularly updated and will be subject to formal annual review by the Data Protection Lead.

5.4 Employees must notify the Data Protection Lead if there are any changes or additions to the data map.

5.5 The data map will be supplemented by an Information Asset Register which will identify the different places in which data is held by CDS, the lead owner of the information asset, its key purpose, location, back up and security arrangements and who may legitimately access the information.

5.6 CDS currently has three privacy notices. One for customers and clients, one for employees and one relating to the work of the CLH Hub for London. The customer privacy notice is available on our website and provided on request to any customer. The employee privacy notice is available on the staff intranet. The CLH Hub for London privacy notice is available on the community led housing London website.

5.7 In addition, as a requirement of our data sharing agreement with Ministry for Levelling Up, Housing and Communities, we provide an additional privacy notice to applicants for housing which covers the data that we collect and share with the Government through the CORE system (COntinuous REcording of Lettings). This privacy notice has also been published on our website as it is applicable to any resident whose tenancy started since 1989.

5.8 We will review and update our privacy notices any time we change our business practices. In addition, there will be a formal review of the privacy notices by the Data Protection Lead annually.

5.9 Where appropriate we will create additional privacy notices in respect to specific categories of data subject where the general customer notice is deemed not applicable.

5.10 CDS uses consent as a ground for processing in only a very limited number of situations where no other ground for processing is available – for example use of photographs, names and stories in newsletters or other marketing materials. In the event that consent is required for the processing of Personal Data, CDS will obtain the consent in writing. The consent provided by the Data Subject must be freely given and the data subject will be required to sign a relevant consent form if willing to consent. Any consent to be obtained by CDS must be for a specific and defined purpose (general consent cannot be obtained).

5.11 **Processing of Special Category Data**

In the event that CDS processes Special Category Personal Data, CDS will do so in accordance with one of the following grounds of processing:

- The data subject has given explicit consent to the processing of this data for a specified purpose;
- Processing is necessary for carrying out obligations or exercising rights related to employment or social security;
- Processing is necessary to protect the vital interests of the data subject or, if the data subject is incapable of giving consent, the vital interests of another person;
- Processing is necessary for the establishment, exercise or defence of legal claims;

- Processing is necessary for reasons of substantial public interest;

- Processing relates to personal data which are manifestly made public by the data subject;

6 Data Protection Impact Assessments

6.1 An assessment of High Risk Data Processing (AHRP) (formarly DPIA) may be required to help identify and minimise the data protection risks of a project.

6.2 An AHRP **must** be conducted for processing that is likely to result in a high risk to individuals such as:

- Systematic and extensive profiling or automated decision making to make significant decisions about people;
- Processing of special category data on a large scale;
- Systematically monitor a publicly accessible place on a large scale (e.g. CCTV systems);
- Processing personal data that could result in a risk of physical harm in the event of a security breach;
- Combine, compare or match data from multiple sources;
- Use profiling, automated decision making or special category data to help make decisions on someone's access to a service, opportunity or benefit

6.3 We will also consider carrying out a AHRP in any other major project involving the use of personal data (using the ICO's AHRP screening checklist). If the use of this checklist identifies the project as one were a AHRP might be appropriate and we decide not to conduct one, we will document our reasons for not doing so.

6.4 If a AHRP is required or we decide to conduct one then it will follow the AHRP process checklist set down by the ICO. It is the responsibility of the Data Protection Lead to decide whether or not a particular processing activity requires a AHRP to be conducted.

6.5 The purpose of a AHRP is to ensure that we have considered the risks related to our intended processing and that we are meeting our broader data protection obligations.

7 Data Sharing

7.1 There are a number of occasions where it will be necessary for CDS to share personal data that it holds. Additionally, we provide managing agent services to a range of housing organisations who will be registered data controllers in their own right.

7.2 For the majority of our managing agent contracts, we will be joint data processors along with the client organisation and our joint obligations will be set out in a formalised addendum to our management agreement.

7.3 Personal data may be shared with local authority partners, repairs contractors, benefit agencies etc. We have set out these circumstances in our privacy statement.

7.4 We will put in place appropriate contractual terms or data sharing agreements with third parties to ensure that the data we may share is only used for the purpose for which it is intended and that the receiving organisation also complies with obligations under the law.

8 Data Storage and Security

8.1 All Personal Data held by CDS will be stored securely, whether electronically or in paper format.

8.2 CDS's main office is in a shared workspace environment which makes data storage and security especially critical.

8.3 Paper Storage

8.3.1 CDS operates in a combination of a shared workspace office environment and home working, which makes the secure storage of Personal & other confidential Data that is on paper especially critical. Information stored on paper should be kept in a secure place where unauthorised personnel cannot access it. Employees should make sure that no Personal Data is left where unauthorised personnel can access it. When the Personal Data is no longer required it must be disposed of by the employee so as to ensure its destruction. If the Personal Data requires to be retained in a physical file then the employee should seek to scan and store it electronically within the CDS's data storage system. Where retention of the paper-based records are required, they will be periodically transferred to secure archive storage and will be retained or destroyed per the criteria set out in our data retention policy.

8.3.2 CDS will operate a clear desk policy within the office environment for any business records.

8.4 Electronic Storage

8.4.1 Personal Data stored electronically must also be protected from unauthorised use and access. Personal Data should be password protected when being sent externally. If Personal data is stored on removable media (CD, DVD, USB memory stick), that removable media must be stored securely at all times when not being used and encrypted to prevent unauthorised access.

8.4.2 Staff should avoid sending personal data internally if it can be shared using other means (e.g. via a shared location on the CDS network). If this is not possible or practicable, personal data can be sent internally without being password protected because CDS's emails are encrypted end-to-end and the data cannot be intercepted at either destination or en route.

8.4.3 Personal Data should not be saved directly to mobile devices or local hard drives on workstations and should be stored in designated servers and secure cloud-based storage systems.

8.4.4 Mobile devices must be password protected to reduce the ability for there to be unauthorised access and will have software installed allowing them to be wiped remotely of data if they are lost or stolen.

9 Breaches

9.1 A data breach can occur at any point when handling Personal Data and CDS has reporting duties in the event of a data breach or potential breach occurring. Breaches which pose a risk to the rights and freedoms of the data subjects who are subject of the breach require to be reported externally in accordance with Clause 9.3 below.

9.2 Internal Reporting

9.2.1 CDS takes the security of data very seriously and in the unlikely event of a breach will take the following steps:

- As soon as the breach or potential breach has occurred, and in any event no later than eight (8) hours after becoming aware it has occurred, the Data Protection Lead must be notified in writing of

  (i) the breach;
  (ii) how it occurred; and
  (iii) what the likely impact of that breach is on any data subject(s);

- CDS will seek to contain the breach by whatever means available;

- The DP Lead must consider whether the breach is one which requires to be reported to the ICO and data subjects affected and do so in accordance with this clause;

- Notify third parties in accordance with the terms of any applicable Data Sharing Agreements

9.3 Reporting to the ICO

The DP Lead will be required to report any breaches which pose a risk to the rights and freedoms of the data subjects who are subject of the breach to the Information Commissioner's Office ("ICO") within 72 hours of the breach occurring. The DP Lead must also consider whether it is appropriate to notify those data subjects affected by the breach.

10 Data Protection Lead (DP Lead)

10.1 The DP Lead has oversight over compliance by CDS with Data Protection laws. The DP Lead details are noted on the CDS website and are contained within the Society's Privacy Notices (Appendix 1)

10.2 The DP Lead will be responsible for:

- monitoring CDS's compliance with Data Protection laws and this Policy;
- co-operating with and serving as CDS's contact for discussions with the ICO;
- reporting breaches or suspected breaches to the ICO and data subjects in accordance with section 9 of this policy

11 Data Subject Rights

11.1 Certain rights are provided to data subjects under the GDPR. Data Subjects are entitled to view the personal data held about them by CDS, whether in written or electronic form.

11.2 Data subjects have a right to request a restriction of processing their data, a right to be forgotten and a right to object to CDS's processing of their data. These rights are set out in CDS's privacy notices and are set out below.

11.3 **Subject Access Requests**

Data Subjects are permitted to view their data held by CDS upon making a request to do so (a Subject Access Request). Upon receipt of a request by a data subject, CDS must respond to the Subject Access Request within one month of the date of receipt of the request. CDS:

- must provide the data subject with an electronic or hard copy of the personal data requested, unless any exemption to the provision of that data applies in law;

- where the personal data comprises data relating to other data subjects, must take reasonable steps to obtain consent from those data subjects to the disclosure of that personal data to the data subject who has made the Subject Access Request; or

- where CDS does not hold the personal data sought by the data subject, must confirm that it does not hold any personal data sought to the data subject as soon as practicably possible, and in any event, not later than one month from the date on which the request was made.

11.4 **The Right to be Forgotten**

11.4.1 A data subject can exercise their right to be forgotten by submitting a request in writing to CDS seeking the erasure of the data subject's Personal Data in its entirety.

11.4.2 Each request received by CDS will be considered on its own merits and legal advice will require to be obtained in relation to such requests from time to time. The DP Lead will have responsibility for accepting or refusing the data subject's request in accordance with clause 11.4 and will respond in writing to the request. The Right to be Forgotten ("Erasure") only applies where:

- The data is no longer necessary in relation to the purpose for which it was collected;
- Where consent is withdrawn;
- Where there is no legal basis for the processing; or
- There is a legal obligation to delete data.

11.5 **The Right to Restrict or Object to Processing**

11.5.1 A data subject may request that CDS restrict its processing of the data subject's Personal Data, or object to the processing of that data.

11.5.2 In the event that any direct marketing is undertaken from time to time by CDS, a data subject has an absolute right to object to processing of this nature by CDS, and if CDS receives a written request to cease processing for this purpose, it will do so immediately.

11.5.3 Each request received by CDS will be considered on its own merits and legal advice will require to be obtained in relation to such requests from time to time. The DP Lead will have responsibility for accepting or refusing the data subject's request in accordance with clause 11.5 and will respond in writing to the request without undue delay but at the latest within one calendar month.

11.5.4 The right to restrict processing can be exercised by a data subject in certain circumstances. When requested and accepted by CDS, it puts limits on what CDS can do with the data. A data subject can request the restriction of processing in the following circumstances:

- If they wish to contest the accuracy of their personal data, whilst CDS verifies the accuracy of the data;
- If CDS's processing is unlawful but the data subject opposes erasure of the data and requests restriction instead;
- If CDS no longer need the data for the purpose of the processing but it is required by the data subject for the establishment, exercise or defence of legal claims; or
- If they have objected to the processing, pending verification of that objection or establishment of whether CDS has legitimate grounds that override the data subject's objection.

11.5.5 If a request to restrict processing is accepted by CDS, steps will be taken to restrict access to the data (by removing it from any public website, temporarily moving the data to another system with restricted access or technical measures to restrict access to the data by users).

11.5.6 If a data subject questions the accuracy of any data or the legitimate grounds for processing the personal data, then CDS will automatically restrict the data whilst these matters are being considered.

11.5.7 In most cases a restriction of processing will only be temporary. If a decision is taken to lift the restriction, CDS will write to the data subject before lifting the restriction.

11.6 **Rectification**

11.6.1 There is an absolute right that allows a data subject to require CDS to rectify any inaccurate personal data concerning a data subject without undue delay.

12 Staff Training and Awareness

12.1 CDS will provide regular training and briefing notes to staff about data protection and confidentiality issues.

12.2 As a minimum, all individuals working for CDS will be required, as part of their induction process, to complete an appropriate e-learning module on GDPR underlying principles and confidentiality in the workplace (the Caldicott Principles).

12.3 Existing staff will be required to undertake refresher GDPR training every other year.

12.4 Whilst the data protection policy and associated policies and processes will always be available on the staff intranet (or equivalent), the data protection policy will be formally circulated to all staff whenever it is updated or formally reviewed and approved by the Board of Management. Staff will be required to confirm in writing that they have read the policy and understood their obligations under it. New staff members will be required to sign the confirmation as part of their induction process.

12.5 We will utilise briefing notes, huddle updates and other appropriate methods of engagement to share with staff data protection best practice, any learning from data protection incidents, etc.

13 Archiving, Retention and Destruction of Data

13.1 CDS cannot store and retain Personal Data indefinitely. It must ensure that Personal data is only retained for the period necessary. CDS has adopted the National Housing Federation's guideline retention periods as set out in Appendix 2.

13.2 CDS will ensure the deletion and/or secure destruction of material that has at the end of the retention period.

13.3 CDS will retain a list of tenancy start and end dates and the name on the rent account after other data is deleted.

14 Acceptable Use Policy

14.1 CDS also has an Acceptable Use Policy which sets out the ground rules for access and use of CDS's Information Technology Systems. Adherence to the Acceptable Use Policy is fundamental to ensuring that the obligations under the Data Protection Policy are also met.

List of Appendices

Appendix 1: Privacy Notices
Appendix 2: Retention Periods

Version control

Date	Amendment	Version control
September 2028	*New policy approved by Board*	*v.1.0*
20.9.2022	*Reviewed and re-approved by Board*	*v1.1*
9.7.2025	*Reviewed by SMT*	*v1.1*
22.9.2025	*After review from IT consultant, minor updates and approved by Board*	*v1.2*