Data Protection Policy

Control information	Control detail
Reference number	CEO/GOV/005/
Version number	4.0
Audience	Public-facing
Effective date	06 August 2026
Review frequency	3 years
Next review date	01 July 2029
Sponsor	Executive Director Corporate Services
Owner	Head of Data & Insight
Author	Data Protection Manager
Consulted stakeholders	Senior Management Team
Approving body	Combined Board
Approval date	03 August 2026
Equality Impact Assessment (EIA) completion date	13 July 2026
Data Protection Impact Assessment (DPIA) completion date	N/A
Applicable Curo strategic objective(s)	☐ Quality Homes ☒ Purposeful Culture ☒ Trusted Customer Services ☐ Collaboration and Growth ☒ Solid Foundations

Control information	Control detail
Applicable legislation, regulations or external standards	• UK GDPR • Data Protection Act 2018 • Data Use and Access Act 2025 • The Privacy and Electronic Communications Regulations 2003 (PECR)
Related internal resources	• Data Retention Policy • Data Retention Schedule • Record of Processing Activity (RoPA) • Data Governance Policy • Curo Code of Conduct • Curo Risk Management & Assurance Framework • ICT Acceptable Use Policy • ICT Acceptable Use Procedure • ICT Equipment Disposal Policy • ICT Equipment Disposal Procedure

Contents

1. Introduction

1.1. Curo's values are Caring, Respectful, Open, Fair and Trusting. We want to ensure that we act, and are seen to act, in line with those values and in the interests of our residents and other service users including colleagues.

1.2. We want to have the necessary policies and procedures in place that demonstrate the highest degree of probity and which reflect our core values.

1.3. We expect members of Curo's Boards of Directors, committees and colleagues to lead by example in following values, requirements, rules, procedures, and practices which protect our integrity. We also expect individuals and organisations associated with Curo (e.g. residents, suppliers, contractors, and service providers) to act in accordance with our values and this includes in respect of data protection.

1.4. For the purposes of this Policy, "Curo" means Curo Group (Albion) Ltd and all subsidiaries from time to time including but not limited to Curo Places Ltd, Curo Choice Ltd, Mulberry Park Community Benefit Society, Curo Enterprises Ltd, Curo Market Rented Services ltd and Curo Finance Ltd.

1.5. Curo acknowledges its responsibilities under UK GDPR (the Retained EU Law version of the General Data Protection Regulation ((EU) 2016/679)), the Data Protection Act 2018, the Data (Use and Access) Act 2025, and the Privacy and Electronic Communications Regulations 2003 (PECR) as amended, replaced or superseded from time to time (together defined in this Policy as 'Data Protection Law').

1.6. This policy covers the processing of all personal data, as defined by Data Protection Law, held by Curo.

1.7. The Chief Executive Officer and the Boards of Directors of Curo are committed to their responsibilities under Data Protection Law.

1.8. The objective of this policy is to protect the rights and freedoms of individuals who are the subject of the personal data we hold, while at the same time being able to lawfully process personal data we hold to meet our strategic priorities. We ensure that personal data is not processed without data subjects' knowledge and, where appropriate, personal data is processed with

consent. To achieve our aim, we will collect and use data fairly, manage it effectively and ensure that our colleagues, contractors, third parties, all relevant bodies and associated persons understand their collective and individual responsibilities.

2. Scope

2.1. This policy covers all processing of 'personal data' held by Curo, including data belonging to customers, clients, suppliers, partners Directors, colleagues and stakeholders and any other personal data from any source. Processing includes anything we do with personal data, including collecting, using, managing, storing, archiving, and disposing of personal data or meta-data. The policy applies to all mediums of data and any means of processing, including (but not limited to) electronic (i.e. by a computer or mobile device), paper, and recordings of images or sound.

2.2. This policy applies to anybody who processes personal data for or on Curo's behalf including: colleagues, volunteers, casual and temporary employees, directors and officers, external organisations employed as processors and any external organisations or individuals with whom we share or disclose personal data. It also applies to current, past and prospective customers and colleagues whose data is processed.

2.3. The policy sets out our principles for processing personal data and how we deliver these principles.

3. Definitions

3.1. **Child:** means anyone under 13 years old.

3.2. **Controller:** means a person or organisation, public authority, agency or other body which, alone or with others, is responsible for determining the purposes and manner in which personal data is processed. Curo is a controller. We may also be a joint controller of personal data with another organisation or person.

3.3. **Criminal Offence Data:** means any data relating to any criminal convictions and offences including anti social behaviour.

3.4. **Data Protection Law:** means the UK GDPR (the Retained EU Law version of the General Data Protection Regulation ((EU) 2016/679)), the Data Protection Act 2018, the Data (Use and Access) Act 2025, and the Privacy and Electronic Communications Regulations 2003 (PECR) as amended, replaced or superseded from time to time.

3.5. **Data Subject:** means any living individual who is the subject of Personal Data held by us.

3.6. **Filing system:** means a structured set of personal data which is accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

3.7. **Personal data:** is as defined by Data Protection Law and means any information relating to an identified or identifiable living individual who can be directly or indirectly identified by reference to an 'identifier' such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that data subject.

3.8. **Personal Data Breach:** means a breach of security or control leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

3.9. **Privacy Notice:** means a notice that communicates to a data subject what data we collect about them, for what reasons, what rights they have over that data, how long we will keep it for and who we might share it with. A Privacy Notice can be a paper or digital document, an audio or visual recording or a verbal description and, regardless of format, the content of which complies with the requirements of Data Protection Law.

3.10. **Processing:** means anything we, and any third party on our behalf, does with personal data we hold from collection through to disposal. It includes how we collect, capture, record, organise, store, adapt, alter, retrieve, consult, use, disclose, disseminate or make available, combine, restrict, erase or destroy personal data. Processing includes automated, electronic, manual and paper based.

3.11. **Profiling:** means the automated processing of personal data intended to evaluate aspects of a living person, or to analyse or predict their performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. A data subject has a right to object to us profiling them as well as a right to be informed if we are profiling them, of measures we are using to do that and the effects of profiling on them.

3.12. **Record of Processing Activity (RoPA):** means the official register of how Curo processes personal data. A RoPA is a requirement under Data Protection Law and summarises what data we hold, why we process it, who we share it with, how long we keep it and the measures we put in place to protect it.

3.13. **Special Categories of personal data:** means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, the processing of genetic data or biometric data in order to uniquely identify the data subject, data concerning health (both mental and physical) or data concerning a data subject's sex life or sexual orientation.

3.14. **Third party:** means a person or organisation, public authority, agency, body, controller, processor or any persons or organisation who are authorised by us to process personal data.

4. External references

4.1. **UK GDPR**

4.2. **Data Protection Act 2018**

4.3. **Data Use and Access Act 2025**

4.4. **The Privacy and Electronic Communications Regulations 2003 (PECR)**

5. Responsibilities

5.1. **The Combined Board and Executive Team:** through the Policy Sponsor, ensures that this Policy delivers Curo's strategic objectives and reflects Curo's values.

5.2. **Policy Sponsor:** Ensures that the policy delivers Curo's strategic objectives and reflects corporate values.

5.3. **Policy Owner:** accountable to the Executive for the effective implementation of this Policy in Curo, so that:

a. The principles are achieved through appropriate team plans and objectives, and

b. Procedures – with appropriate RACIs – translate the policy and objectives into practice.

5.4. **The Chief Executive:** has a statutory responsibility for compliance with legislation. They also lead the development of an organisational culture in which this Policy can operate effectively.

5.5. **Executive Director Corporate Services:** is accountable for the delivery of the policy objectives across Curo. The Privacy Team is responsible for the day to day management of data protection issues, including the provision of advice to colleagues.

5.6. **The Data Protection Officer (DPO):** is responsible for monitoring Curo's compliance with Data Protection Law, informing and advising on Curo's data protection obligations under Data Protection Law, advising on Data Protection Impact Assessments (DPIAs) and acting as the primary point of contact for individuals and for the data protection regulator, the Information Commission (IC).

5.7. **All Executive Directors and Directors:** are accountable for ensuring compliance with this policy in their service areas. This includes developing and encouraging good information handling practices within Curo and ensuring the RoPA is kept accurate and up to date in their service area.

5.8. **The Data Protection Officer and Directors:** will ensure all relevant information about data processing is communicated to all colleagues and relevant third parties and shall ensure awareness and understanding is measured and reported periodically.

5.9. **The Director of Technology:** is responsible for ensuring appropriate levels of cyber security is applied to all digital personal data held by Curo in centrally managed IT systems and has an appropriate level of cyber security applied to it.

5.10. **All Managers:** are responsible for delivering operational processes, and compliance, within their teams.

5.11. **All colleagues, Board Directors and committee members:** are responsible for respecting privacy and confidentiality in accordance with this Policy and Data Protection Law. Breaches of any Curo policy or procedure may be investigated under the Disciplinary Policy and/or the Curo Code of Conduct.

5.12. **Involved Residents, partners, processors and any third parties:** working with or for Curo, and who have, or may have access to personal data, are required to have read, understood and comply with this Policy.

6. Principles

6.1. As a data controller, Curo acknowledges the right of all individuals to have personal information processed in accordance with Data Protection Law and we endorse the following Principles relating to processing of personal data:

a. **Lawful, fair and transparent:** Personal data is processed in a way that is lawful, fair and transparent in relation to the data subject;

b. **Purpose limitation:** Personal data is collected only for specified, explicit and legitimate purposes and is not further processed in a manner different to those specified purposes;

c. **Data minimisation:** Personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;

d. **Accuracy:** Personal data is accurate and kept up to date;

e. **Storage limitation:** Personal data is stored in a form which allows identification of data subjects for no longer than is necessary for the purposes for which personal data is processed;

f. **Integrity and confidentiality:** Personal data is processed in a manner that ensures appropriate security, technical or organisational measures;

g. **Accountability:** Compliance with Data Protection Law can be demonstrated by appropriate documentation of the processing of personal data; and

h. **Territory:** Personal data is not transferred outside the UK without adequate protection.

6.2. Curo recognises the legal rights of the data subjects whose personal data it is processing, or intends to process, and ensures that data subjects are appropriately advised of their rights as follows:

a. **Informed:** Data subjects have the right to be told what personal data we have relating to them, for what purposes, how long we will keep it and who we might share it with;

b. **Access:** Data subjects have the right to request a copy of their personal data, subject to specific legal exemptions;

c. **Portability:** Data subjects have the right to request that their personal data is provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller;

d. **Erasure:** Data subjects have the right to request that their personal data is erased;

e. **Restriction:** Data subjects have the right to request that any or all processing of their personal data is restricted. Processing will be suspended until the processing in question has been resolved or the restriction has been lifted;

f. **Rectification:** Data subjects have the right to have any incorrect or incomplete information rectified;

g. **Objection:** Data subjects have the right to request for an objection to be lodged to any processing undertaken by Curo involving their own data, including marketing, automated decisions and profiling. Processing will be suspended until the objection is resolved;

h. **Automated decision making and profiling:** Data subjects have the right to be informed about any processing involving an automated decision-taking process that will significantly affect them, and the right to request a meaningful human review of a decision made solely by an automated process;

i. **Complaint:** Data Subjects have the right to lodge a complaint with Curo about any dissatisfaction regarding how we handle their personal data. This might include:

- how their request for access to data or their right to erasure has been handled; or
- concerns that their personal data has been lost, stolen or inadequately secured.

j. **Escalation to the Information Commission:** If having lodged a complaint with Curo, a data subject remains dissatisfied with our response, they have the right to escalate to the Information Commission; and

k. **Compensation:** Data Subjects have the right to sue Curo for compensation if they suffer damage caused by Curo's contravention of Data Protection Law;

6.3. We recognise that unlawful processing of personal data, including its sale where this has not been authorised by the data subject, is a criminal offence.

6.4. We support colleagues by providing training, up to date guidance, and advice.

6.5. We recognise that individuals may exercise their data protection rights either directly or through someone acting on their behalf. We will accept requests made by such a representative where we are satisfied that they have appropriate authority to act on behalf of the data subject for example a Lasting Power of Attorney. Where a person lacks capacity to exercise their rights, we will accept requests from someone who has the legal authority to act on their behalf or who is otherwise authorised to do so in their best interests.

7. Application

7.1. Curo's data protection procedures deliver the principles of this policy and ensure:

a. **Fairness and transparency:** when collecting personal data we provide data subjects with an appropriate Privacy Notice which explains who we

are, the purposes for which we will use the data collected, how long we will retain it and who we might share the data with.

b. **Lawfulness:** all personal data will be collected according to the lawful ground specified for the data processing activities described in the Record of Processing Activity (RoPA). Each Director is accountable for ensuring that there are lawful grounds for all data processing activities that fall under their sphere of control.

c. **Data processing purposes:** Data obtained for specified purposes is not used for any purpose that differs from those described in Curo's Privacy Policies and the RoPA.

d. **Data minimisation:** Curo uses a minimum of personal data in its data processing activities and periodically reviews the relevance of the information that it collects. Directors are accountable for ensuring that no unnecessary, irrelevant or unjustifiable personal data is collected or created either directly or indirectly through the data processing activities they are responsible for and/or engage in.

e. **Data quality:** Curo recognises that the accuracy of data is important, and that some data is more important to keep up to date than others. Directors are accountable for maintaining data as accurate and up to date as possible, in particular data which would have a detrimental impact on data subjects if it were inaccurate or out of date. Any personal data that cannot reasonably be assumed to be accurate and up-to-date must be updated, erased or anonymised.

f. **Data retention:** Through our Data Retention Schedule we ensure that we do not retain personal data for any longer than is necessary for legal or regulatory reasons or for its legitimate organisational purposes. We ensure timely and appropriate disposal at the end of data's useful life through risk-assessed measures such as erasure or anonymisation. No data is kept unless it is reasonable to assume that it is accurate.

Data Subject Rights

7.2. All colleagues are responsible for ensuring that individuals are clearly and accurately informed about how their personal data is used for example by providing a copy of the appropriate Privacy Notice.

7.3. All colleagues are responsible for recognising a Data Subject Rights request and reporting it immediately to the Privacy Team at privacy@curo-group.co.uk without delay.

7.4. The Data Protection Manager is responsible for overseeing all Data Subject Rights requests and complaints and ensuring response times are within the prescribed time frames.

Consent

7.5. Consent is only relied on in limited circumstances. Where consent is relied upon, consent to process personal data and when appropriate, Special Categories of personal data, is obtained by Curo using standard consent documents e.g. during induction for participants on programmes.

7.6. Where consent is relied upon as a lawful ground for processing personal data the data subject must been fully informed of the intended processing and will have signified their agreement to the intended processing. Their agreement must be:

a. explicitly and freely given;

b. specific; and

c. informed and an unambiguous indication of their wishes;

7.7. The consent given by the data subject must be:

a. by statement or by a clear affirmative action;

b. signifying agreement to us processing their personal data;

c. informed that they can withdraw their consent at any time; and

d. documented as obtained and refreshed appropriately by us.

7.8. For Special Categories of personal data explicit consent of the data subject must be obtained unless an alternative lawful basis for processing exists.

Information Security

7.9. Information security is essential to protecting the rights and freedoms of data subjects and to enable us to process personal data lawfully and effectively.

7.10. Any personal data processed by us or on our behalf is processed with the appropriate security measures in place, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. The ICT Acceptable Use Policy and Procedure sets out expectations of all colleagues in maintaining personal data security.

Data Protection Impact Assessments

7.11. Data Protection Impact Assessments are conducted as appropriate, taking into account all the circumstances of Curo's controlling or processing operations in compliance with the Data Protection Impact Assessment (DPIA) Procedure.

8. Security of data

Sharing Data

8.1. All colleagues must ensure that any personal data that Curo holds and for which they are responsible is kept securely. We only share personal data where it is lawful, necessary and proportionate to do so. One-off disclosures may be made in urgent circumstances, for example where there is an immediate risk to an individual's safety or a statutory requirement to share information without delay. Where data is shared on an ongoing or routine basis with a third party, an appropriate formal arrangement will be put in place, such as a Data Sharing Protocol, Data Processing Agreement or Data Sharing Agreement. These arrangements set out the required security, confidentiality and compliance standards to ensure personal data remains protected and complies with data protection requirements. If a colleague is unsure about sharing personal data, they should refer to the Privacy Team for advice.

Data Security

8.2. Colleagues may only access personal data if they need to use it in relation to their role, and access is granted on this basis. All colleagues are expected to treat all personal data with the highest security and to ensure it is kept securely at all times (refer to the ICT Acceptable Use Policy and Procedure).

Data Breaches

8.3. Curo has a legal duty to report some personal data breaches 'without delay' to the relevant authority, and in certain circumstances, to the data subject. If you discover or believe a data breach has occurred this must be notified to the Privacy Team **immediately** using the appropriate data breach form.

9. Retention and disposal of data

9.1. Curo does not keep personal data in a form that permits identification of data subjects for any longer than is necessary, in relation to the purpose(s) for which the data was originally collected as defined in the Data Retention Schedule.

9.2. The retention period for each category of personal data is defined in the Record of Processing Activity (RoPA) along with the criteria used to determine this period including any statutory obligations Curo has to retain the data. This is defined in the Data Retention Schedule.

9.3. Personal data is securely destroyed or erased when no longer required using appropriate technical and organisational measures that protect its confidentiality and the rights and freedoms of individuals.

10. Data Transfers

10.1. Personal data may only be transferred outside the UK where the destination country has been granted UK adequacy regulations or where appropriate safeguards are in place in accordance with Data Protection Law. Any international transfer must be approved by the DPO and carried out in compliance with Data Protection Law.

11. Risks associated with the processing of particular types of personal data

11.1. Curo recognises that certain types of personal data processing can create risks to the rights and freedoms of individuals, particularly where Special Category Data and/or Criminal Offence Data is involved. We assess these risks as part of our planning and decision-making processes.

11.2. A Data Protection Impact Assessment (DPIA) is undertaken whenever processing is likely to result in a high risk to individuals, in accordance with the requirements of the UK GDPR. This includes new processing activities, significant changes to existing processing, where new technologies or large-scale processing activities are proposed and any processing carried out on our behalf by external organisations where the nature of the activity may present a high risk.

11.3. The DPIA process helps us identify, analyse and mitigate risks before the processing begins. It ensures that appropriate safeguards are built into the design of systems, services and processes in good time, and that any residual risks are understood and managed. A DPIA template and supporting questions and guidance ensures assessments are completed consistently and to an appropriate standard. A DPIA register records all completed assessments.

11.4. No high-risk processing will commence until a DPIA has been completed and any necessary risk-mitigation measures have been agreed and implemented. Where a DPIA indicates that risks cannot be mitigated to an acceptable level, the DPO will consult the Information Commission before proceeding.

Version control

Version number	Update type	Update summary	Updated by	Update date
1.0	Full review	• First version created		
2.0	Full review	• Post GDPR – reviewed and updated	Director of Governance	July 2020
3.0	Full review	• Reviewed and updated	Director of Governance	July 2023
4.0	Full review	• Transfer of relevant content to updated policy template. • Bringing content in line with regulatory guidance and legislative changes. • Emphasising the advisory and monitoring role of the Data Protection Officer.	Data Protection Manager	03 July 2026