

Data Protection Policy

**Policy Owner:**

**Executive Director Finance and Strategy**

**Accountable Lead: Director of Governance**

1. [Policy Statement and aims 3](#_bookmark0)
2. [Scope 4](#_bookmark1)
3. [Definitions 4](#_bookmark2)
4. [Roles and responsibilities 6](#_bookmark3)
5. [Principles 6](#_bookmark4)
6. [Application 8](#_bookmark5)
7. [Security of data 10](#_bookmark6)
8. [Retention and disposal of data 11](#_bookmark7)
9. [Data transfers 11](#_bookmark8)
10. [Risks associated with the processing of particular types of personal data 11](#_bookmark9)

|  |  |
| --- | --- |
| **Policy Control** | |
| **Policy Level** | Statutory and Regulatory |
| **Policy Owner** | Director of Governance |
| **Policy Reference** | **CEO/GOV/005/** |
| **Link to Strategy** | Linked to all Curo Strategies |
| **Version Control** | V2 (post GDPR) – reviewed and updated July 2020 V3 – reviewed and updated July 2023 |
| **Approved by** | Combined Board September 2023 |
| **Consultation** | Director ICT  Director of Governance  Data Protection People (independent DP advisers) |
| **Equality analysis** | Equalities Impact Assessment completed and no remedial actions identified |
| **Next review date** | July 2026 |
| **Associated Policies & Procedures and other documents** | * Data Retention Schedule * Information Asset Registers * Code of Conduct * Risk Management Policy * ICT Acceptable Use Policy and Procedure * ICT Equipment Disposal Policy and Procedure |

# Policy Statement and aims

Curo is an organisation where respect, integrity and honesty are core values. We want to ensure that we act, and are seen to act, wholly in the interests of our residents and other service users including colleagues.

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

We expect Members and colleagues to lead by example in following 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 adhere to the same principles.

Curo Group, and its member organisations, acknowledge their responsibilities under the (Retained EU Legislation) Regulation (EU) 2016/679 (UK General Data Protection Regulation) (GDPR) and the *Data Protection Act 2018* (DPA).

This policy covers the processing of all personal data, as defined by Data Protection Law, held by Curo. Curo Group shall mean 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 Enterprise Ltd and Curo Market Rented Services ltd

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

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.

Controls and measures to achieve this aim are described by this policy and connected processes, procedures and guidance documents (collectively referred to as the ‘Data Protection Manual’).

# Scope

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

# Definitions

* 1. This policy contains a number of terms, which are defined in accordance with Article 4; GDPR and/or DPA and as set out below:
* **Data Protection Law** means the General Data Protection Regulation and the Data Protection Act 2018 and any laws amending, enacting, consolidating, replacing or superseding the GDPR or DPA or otherwise introducing obligations in respect of data protection in the UK.
* **Data Subject** means any living individual who is the subject of personal data held by us.
* **Personal data** 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.
* **Special categories of personal data** means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and 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.
* **Criminal Data** means any data relating to any criminal convictions and offences including anti social behaviour
* **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.

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

# Roles and responsibilities

* 1. The Combined Board and Executive Team, through the Policy Owner, ensures that the policy delivers Curo’s strategic objectives and reflects corporate values. The Accountable Lead is accountable to the Executive for the effective implementation of the policy in Curo, so that:
* The principles are achieved through appropriate team plans and objectives, and
* Procedures – with appropriate RACIs – translate the policy and objectives into practice.
  1. 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.
  2. The Director of Governance is accountable for the delivery of the policy objectives across Curo. The Governance team are responsible for the day to day management of data protection issues, including the provision of advice to colleagues.
  3. The Data Protection Officer is accountable for ensuring that Curo complies with Data Protection Law, informing and advising on the protection of personal data in relation to Data Protection Law and responding to all reported data breaches or suspected data breaches. The Data Protection Officer is responsible for reviewing Curo’s processing activities annually, authorising new processing and any other requirements included in the Data Protection Manual.
  4. All Executive Directors and Directors are accountable for applying this policy in their service areas. They are also accountable for developing and encouraging good information handling practices within Curo, documenting the ways personal data is processed within their service area and for ensuring compliance with this policy, as well as the procedures and guidance documents within the Data Protection Manual.
  5. The Data Protection Officer and each 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.
  6. The Director of ICT 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.
  7. All Managers are responsible for delivering operational processes, and compliance, within their teams.
  8. All colleagues and Board Directors are responsible for respecting privacy and confidentiality in accordance with this policy and Data Protection Law. A breach of any data protection policy or procedure may also be investigated under the Disciplinary Policy.
  9. 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.

# Principles

* 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:
* **Lawful, fair and transparent**: Personal data is processed in a way that is lawful, fair and transparent in relation to the data subject;
* **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;
* **Data minimisation**: Personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
* **Accuracy**: Personal data is accurate and kept up to date;
* **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;
* **Integrity and confidentiality**: Personal data is processed in a manner that ensures appropriate security, technical or organisational measures;
* **Accountability:** Compliance with Data Protection Law can be demonstrated by appropriate documentation of the processing of personal data; and
* **Territory:** Personal data is not transferred outside of the UK without adequate protection.
  1. 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. Curo recognises that data subjects have the following rights regarding data processing and the personal data that is recorded about them:
* **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;
* **Access**: Data subjects have the right to be provided with any and all information held about them;
* **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;
* **Erasure:** Data subjects have the right to request that their personal data is erased;
* **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;
* **Rectification:** Data subjects have the right to have any incorrect or incomplete information rectified;
* **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;
* **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 have any decision made solely by an automated process reviewed;
* **Complaint**: Data Subjects have the right to lodge a complaint with Curo about:
  + how their personal data has been processed;
  + how their request for access to data has been handled;
  + how their complaint has been handled; and
  + appeal against any decision made following a complaint.
* **Complaint to Information Commissioner’s Office**: Data Subjects have the right to lodge a complaint with the Information Commissioner’s Office to assess whether any provision of Data Protection Law has been contravened; and
* **Compensation:** Data Subjects have the right to sue Curo (or our contractors, suppliers or partners) for compensation if they suffer damage by any contravention of Data Protection Law;
  1. Where the right of a data subject is a right to request some action, the presumption is that all requests will be accepted and actioned. All requests and rights will be resolved in accordance with the requirements of Data Protection Law. The Data Protection Manual describes the procedures for processing any such request, including the conditions that would overturn the presumption that we will accept and action any rights request. Where a request is not accepted or actioned, the data subject will be informed about the reasons.
  2. 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.
  3. We support colleagues by providing training, up to date guidance, and advice.
  4. We will act in accordance with the requirements of the *Mental Capacity Act 2005* recognising the right of those without mental capacity to be able to authorise a request to access personal data by an attorney or appointed person in making a request on their behalf.

# Application

## Information Asset Register

Curo maintains an Information Asset Register and an analysis of data flows as part of its approach to address risks and opportunities involving personal data. Curo’s Information Asset Register describes:

* departmental processes that use personal data;
* source(s) and descriptions of personal data;
* volume of data subjects;
* description of each item of personal data;
* processing activity;
* an inventory of data categories of personal data processed;
* the purpose(s) for which each category of personal data is used;
* recipients, and potential recipients, of the personal data;
* the role of Curo throughout the data flow;
* key systems and repositories;
* any data transfers; and
* all retention and disposal requirements.
  1. Curo’s data protection procedures deliver the principles of this policy and ensure:
* **Fairness and transparency:** when collecting personal data we provide the 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.
* **Lawfulness:** all personal data will be collected according to the lawful ground specified for the data processing activities described in the Information Asset Register. Each Head of Service is accountable for ensuring that there are lawful grounds for all data processing activities that fall under their sphere of control and that each lawful ground is documented as required by the Data Protection Manual.
* **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 Information Asset Register.
* **Data minimisation:** - Curo uses a minimum of personal data in its data processing activities and periodically reviews the relevance of the information that is 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.
* **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 is updated, erased or anonymised.
* **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

* + 1. Directors are responsible for ensuring that the correct Privacy Notice is available for each use of data.
    2. All colleagues are responsible for ensuring that the appropriate information is given to each data subject at the time of collecting the personal data.
    3. All colleagues are responsible for recognising a Data Subject Rights request and reporting it immediately to the Data Protection Officer without delay.
    4. The Data Protection Officer is accountable for dealing with all Data Subject Rights requests and complaints and responding within the time frame prescribed by Data Protection Law. See the Data Subject Access Request procedure.

## Consent

* + 1. 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.
    2. 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:
       - explicitly and freely given;
       - specific; and
       - informed and an unambiguous indication of their wishes;
    3. The consent given by the data subject must be:
       - by statement or by a clear affirmative action;
       - signifying agreement to us processing their personal data;
       - informed that they can withdraw their consent at any time; and
       - documented as obtained and refreshed appropriately by us.
    4. For Special Categories of personal data explicit consent of the data subject must be obtained unless an alternative lawful basis for processing exists. Guidance on this is provided by the Governance Team.
    5. If Curo provides online services to children, parental or custodial authorisation is obtained. This requirement applies to children under the age of 13.

## Information Security

* + 1. Information security is essential to protecting the rights and freedoms of data subjects and to enable us to process personal data lawfully and effectively.
    2. 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

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.

# Security of data

## Sharing Data

All colleagues must ensure that any personal data that Curo holds and for which they are responsible is kept securely. Personal data must not be disclosed to any third party unless that third party has been specifically authorised to receive that information and has entered into a contract or Data Sharing Agreement. If you are unsure about sharing personal data please speak with your Head of Service or the Data Protection Officer, and refer to the Data Sharing Procedure.

## Data Security

Colleagues may only access personal data if they need to use it, 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. [See the ICT Acceptable Use Policy and Procedure]

We have a legal duty to report 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 Data Protection Officer **immediately** using the Personal Data Breach Notification Procedure.

# Retention and disposal of data

* 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.
  2. The retention period for each category of personal data is defined in the Information Asset Register 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.
  3. Personal data is disposed of securely in accordance with the sixth principle of the GDPR – processed in an appropriate manner to maintain security, thereby protecting the “rights and freedoms” of data subjects. Any disposal of hardware is performed in accordance with the ICT Equipment Disposal Policy and Procedure.

# Data transfers

* 1. Transfer of personal data to non-European Economic Area (EEA) countries is prohibited by Data Protection Law, unless the non-EEA country has an adequate level of protection or there are additional safeguards in place. Transfer of personal data to a non-EEA country may only be made with the agreement of the Data Protection Officer and Director of Governance and in accordance with Data Protection Law.

# Risks associated with the processing of particular types of personal data

* 1. Curo is aware of the risks associated with the processing of particular types of personal data. Curo assesses the level of risk to data subjects associated with the processing of their personal data. Data Protection Impact Assessments are conducted in relation to the processing of personal data by Curo, and in relation to processing undertaken by other organisations on behalf of Curo in compliance with the Data Protection Impact Assessment (DPIA) Procedure.
  2. Curo manages any risks identified by the risk assessment to reduce the likelihood of a non- conformance with this policy according to the Group’s Risk Management Policy.
  3. Where a type of processing (in particular using new technologies and taking into account the nature, scope, context and purposes of the processing) is likely to result in a high risk to the rights and freedoms of natural persons, prior to processing Curo conducts a DPIA of the impact of the envisaged processing operations. A single DPIA may address a set of similar processing operations that present similar high risks.
  4. Where, as a result of a DPIA (see paragraph 6.6) it is clear that Curo is about to commence processing of personal data that could cause damage and/or distress to data subjects, the decision as to whether or not Curo may proceed is escalated for review to the Data Protection Officer.
  5. When there are significant concerns, either as to the potential damage or distress, or the quantity of data concerned, the Data Protection Officer escalates the matter to the Information Commissioner’s Office.
  6. Appropriate controls are selected and applied to reduce the level of risk associated with

processing individual data to an acceptable level, by reference to Curo’s risk appetite and the requirements of Data Protection Law. This is recorded in the risk registers as necessary in line with the Group’s Risk Management Policy.