

Cambridgeshire Community Foundation

Policy Number	Name of Policy	Owned by	Applies to
CCF/GOV/002	Data Protection policy	CEO	Whole Organisation
Review Date	Reviewed by	Frequency of Review	Next Review Date
May 2026	HR&Gov committee	Annually	May 2027

Data Protection Policy

1.0 Introduction

1.1 Cambridgeshire Community Foundation (CCF) is committed to complying with privacy and data protection laws, including:

- the UK General Data Protection Regulation (UK GDPR) as retained in UK law by the European Union (Withdrawal) Act 2018, and the Data Protection Act 2018 (DPA 2018)
- all other applicable UK laws and regulations relating to the processing of personal data and privacy, including the Data (Use and Access) Act 2025 (DUAA 2025), statutory instruments, and, where applicable, the guidance and codes of practice issued by the Information Commissioner's Office (ICO).

This policy sets out how we protect individuals' personal data.

1.2 Anyone who handles personal data on behalf of CCF must ensure that we comply with this policy. Any breach of this policy will be taken seriously and may result in disciplinary action or more serious sanctions.

1.3 The types of personal data that we may handle include details of grant applicants, beneficiaries, donors, staff, trustees, volunteers and other stakeholders.

1.4 Any questions or concerns about this policy should be referred in the first instance to Viv Atkinson (viv@cambscf.org.uk), who is the Data Protection Officer at CCF. The person with overall responsibility for compliance with the UK GDPR, DPA 2018 and this policy is Michael O'Toole, CEO.

1.5 The Data (Use and Access) Act 2025 (DUAA 2025) received Royal Assent on 19 June 2025 and introduces changes to the UK data protection framework that will affect how CCF processes personal data. The Act is being commenced in stages throughout 2026, with specific provisions taking effect at different times as commencement orders are made. This policy will be updated as those provisions come into force. In the meantime, CCF will monitor the ICO's implementation guidance and ensure that any required changes to its practices and documentation are implemented throughout 2026 as the relevant provisions are commenced.

Cambridgeshire Community Foundation

2.0 Definitions

- 2.1 **Data Subjects** include all living individuals about whom we hold personal data, for instance an employee or a supporter. All data subjects have legal rights in relation to their personal data.
- 2.2 **Personal Data** means any information relating to a living person who can be identified directly or indirectly from that information (or from that information and other information in our possession). Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as performance appraisal). It can also include an identifier such as an identification number, location data, an online identifier specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. It can also include photographs and case study material
- 2.3 **Data Controllers** are the people who, or organisations which, decide the purposes and the means for which any personal data is processed. They have a responsibility to process personal data in compliance with the Legislation. CCF is the data controller of all personal data that we manage in connection with our work and activities.
- 2.4 **Data Processors** include any persons who process personal data on behalf of a data controller. Employees of data controllers are excluded from this definition, but it could include other organisations, such as website hosts or service providers, that handle personal data on our behalf.
- 2.5 **Restricted Transfer** means a transfer of personal data to a country or territory outside the United Kingdom, or to an international organisation, that is not covered by a UK adequacy regulation made under section 17A DPA 2018. Where a restricted transfer is necessary, CCF will ensure that an appropriate safeguard is in place, such as the International Data Transfer Agreement (IDTA) or the Addendum to EU Standard Contractual Clauses.
- 2.6 **ICO** means the Information Commissioner's Office (the authority which oversees data protection regulation in the UK).
- 2.7 **Processing** is any activity that involves use of personal data, whether or not by automated means. It includes but is not limited to the following in relation to personal data:
- collecting
 - recording
 - organising
 - structuring
 - storing
 - adapting or altering

Cambridgeshire Community Foundation

- retrieving
- disclosing by transmission
- disseminating or otherwise making available
- aligning or combining
- restricting
- erasing
- destruction.

2.8 **Special Category Data** is the term used in the UK GDPR (Article 9) for categories of personal data that warrant higher protection because of their sensitivity. This replaces the older term “sensitive personal data” used in the Data Protection Act 1998. It includes information about a person’s:

- racial or ethnic origin
- political opinion
- religious, philosophical or similar beliefs
- trade union membership
- physical or mental health or condition
- sexual life or orientation
- genetic data
- biometric data

3.0 Data Protection Principles

Anyone processing personal data must comply with the six data protection principles set out in Article 5 UK GDPR. CCF is required to comply with these principles and to demonstrate that compliance (the accountability principle) in respect of any personal data we process as a data controller.

Personal data should be:

1. processed fairly, lawfully and transparently
2. collected for specified, explicit and legitimate purposes and not further processed in a way which is incompatible with those purposes
3. adequate, relevant and limited to what is necessary for the purpose for which it is held
4. accurate and, where necessary, kept up to date
5. not kept longer than necessary
6. processed in a manner that ensures appropriate security of the personal data.

3.1 Processing data fairly and lawfully

3.1.1 The first data protection principle requires that personal data is obtained fairly and lawfully and processed for purposes that the data subject has been told about. Processing will only be lawful if certain conditions are satisfied, including where the data

Cambridgeshire Community Foundation

subject has given consent or where the processing is necessary for one or more specified reasons, such as the performance of a contract.

3.1.2 To comply with this principle, every time we receive personal data about a person directly from that individual, which we intend to keep, we shall provide that person with 'the fair processing information'. In other words, we shall tell them:

- the type of information we will be collecting (categories of personal data concerned)
- that CCF will be holding their information together with the contact details of CCF's Data Protection Officer
- why we are collecting their information and what we intend to do with it, for instance, to process donations, assess eligibility for grants or issue mailing updates about our activities
- the legal basis for collecting their information (for example, we are relying on their consent, on our legitimate interests or on another legal basis)
- if we are relying on legitimate interests as a basis for processing, what those legitimate interests are
- whether the provision of their personal data is part of a statutory or contractual obligation, and details of the consequences of the data subject not providing that data
- the period for which their personal data will be stored or, where that is not possible, the criteria that will be used to decide that period
- details of people or organisations with whom we will be sharing their personal data
- if relevant, the fact that we will be making a restricted transfer of their personal data outside the UK and details of the appropriate safeguards in place (such as a UK adequacy regulation, IDTA or SCCs Addendum)
- the existence of any automated decision-making, including profiling, in relation to that personal data.

3.1.3 Where we obtain personal data about a person from a source other than the person themselves, we shall provide that individual with the following information in addition to that listed under 3.1.2 above.

- the categories of personal data that we hold
- the source of the personal data and whether this is a public source.

In both scenarios (where personal data is obtained directly or indirectly), we shall also inform individuals of their rights outlined in section 3.5 below, including the right to lodge a complaint with the ICO and the right to withdraw consent to the processing of their personal data.

3.1.4 This fair processing information can be provided in a number of places, including on our website, in mailings or on application forms. We shall ensure that the fair processing of information is concise, transparent and easily accessible.

3.2 Processing data for the original purpose

The second data protection principle requires that personal data is processed only for specific, explicit and legitimate purposes that the individual was informed about when we first obtained their information. We shall not collect personal data for one purpose and then use it for another incompatible purpose. If it becomes necessary to process personal data for a new purpose, CCF will first assess whether that new purpose is compatible with the original purpose (taking into account the factors in Article 6(4) UK GDPR).

If the new purpose is not compatible, CCF will identify a fresh lawful basis before proceeding and will provide the individual with updated fair processing information. Consent will be sought where it is the most appropriate basis but is not the only available route to processing data for a new purpose.

3.3 Personal data should be adequate and accurate

The third and fourth data protection principles require that the personal data we keep should be accurate, adequate and relevant. Data will be limited to what is necessary in relation to the purposes for which it is processed. Inaccurate or out-of-date data will be destroyed securely, and we will take every reasonable step to ensure that any inaccurate personal data is corrected.

3.4 Not retaining data longer than necessary

The fifth data protection principle requires that we should not keep personal data for longer than we need to for the purpose for which it was collected. This means that the personal data we hold will be destroyed or erased from our systems when it is no longer needed, which is normally for a maximum of 6 years after our relationship with an individual has ceased. However, we are occasionally required to hold data for longer periods for specific programmes – see data retention schedule (CCF-Gov-002A)

3.5 Rights of individuals under the UK GDPR, DPA 2018 and DUAA 2025

The UK GDPR gives people rights regarding how organisations process their personal data. Everyone who holds personal data on behalf of CCF needs to be aware of these rights. The rights include:

- to request a copy of any personal data that we hold about them (as data controller), as well as a description of the type of information that we are processing, the uses that are being made of the information, details of anyone to whom their personal data has been disclosed, and how long the data will be stored (known as subject access rights)

Cambridgeshire Community Foundation

- to be told, where any information is not collected from the person directly, any available information as to the source of the information
- to be told of the existence of automated decision-making
- to object to the processing of data where the processing is based on either the conditions of public interest or legitimate interests
- to have all personal data erased (the right to be forgotten) unless certain limited conditions apply
- to restrict processing where the individual has objected to the processing
- to have inaccurate data amended or destroyed
- to data portability. Where processing is based on consent or contract and carried out by automated means, to receive a copy of their personal data in a structured, commonly used and machine-readable format, and to have that data transmitted to another controller (Article 20 UK GDPR)
- not to be subject to a decision based solely on automated processing (including profiling) which produces legal or similarly significant effects. Where such processing occurs, the data subject has the right to request human review of the decision, to express their point of view, and to contest the decision (Article 22 UK GDPR. Data (Use and Access) Act 2025, ss.11–14).

3.6 Data security

- 3.6.1 The sixth data protection principle requires that we keep secure any personal data that we hold. We are required to put in place procedures to keep the personal data that we hold secure, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- 3.6.2 When we are dealing with sensitive personal data, more rigorous security measures are likely to be needed, for instance, if sensitive personal data (such as details of an individual's health, race or sexuality) is held on a memory stick or other portable device it should always be encrypted.
- 3.6.3 The following security procedures and monitoring processes must be followed in relation to all personal data processed by us: measures to restore availability and access to data in a timely manner in the event of a physical or technical incident; process for regularly testing, assessing and evaluating effectiveness of security measures; backing up data; ensuring that individual monitors do not show confidential information to passers-by and that staff log off from their PC when it is left unattended; personal data must always be transferred in a secure manner; desks and cupboards should be kept locked if they hold confidential information of any kind and staff must keep data secure when travelling or using it outside the office.

4.0 Restricted Transfers (transferring data outside the UK)

The UK GDPR (Chapter V) and DPA 2018 restrict the transfer of personal data to countries or territories outside the UK unless adequate protection is in place. CCF will only make a restricted transfer where one of the following applies:

- (a) the destination country or territory is covered by UK adequacy regulations
- (b) appropriate safeguards are in place, such as an International Data Transfer Agreement (IDTA) or the UK Addendum to EU Standard Contractual Clauses (SCCs) or
- (c) a specific derogation under Article 49 UK GDPR applies.

CCF will carry out a Transfer Risk Assessment (TRA) where required before making a restricted transfer.

5.0 Links to other websites

Our website may contain links to other websites of interest. However, once these links have been used to leave our site, we have no control over the other website. Therefore, we cannot be responsible for the protection and privacy of any information provided whilst visiting such sites which are not governed by this policy.

6.0 Processing sensitive personal data

On some occasions, we may collect special category data (as defined in section 2.8). Processing of special category data is prohibited unless one of the conditions in Article 9(2) UK GDPR is met and, where required, a further condition under Schedule 1 DPA 2018 is also satisfied.

The conditions most likely to be relevant to CCF include:

- explicit consent of the data subject
- processing necessary for the purposes of carrying out obligations or exercising rights in the field of employment, social security or social protection law
- processing necessary for reasons of substantial public interest
- and processing necessary for the establishment, exercise or defence of legal claims.

CCF will identify and record the applicable condition before processing any special category data and will maintain an Appropriate Policy Document where required by Schedule 1 of the DPA 2018.

7.0 Notification

Cambridgeshire Community Foundation

- 7.1 CCF is required to pay the annual data protection fee to the ICO and to keep its registration details up to date. Where we intend to carry out processing that is likely to result in a high risk to individuals' rights and freedoms (for example, large-scale processing of special category data or systematic monitoring), we will carry out a Data Protection Impact Assessment (DPIA) before commencing that processing, in accordance with Article 35 UK GDPR. Where the DPIA indicates a high residual risk that cannot be mitigated, we will consult the ICO before proceeding (Article 36 UK GDPR).
- 7.2 We will report breaches (other than those which are unlikely to be a risk to individuals) to the ICO when necessary, within 72 hours. We will also notify affected individuals where the breach is likely to result in a high risk to the rights and freedoms of these individuals.

8.0 Managing a data breach

- 8.1 A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches resulting from both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

8.2 *Responsibility*

All staff and associated personnel (whether contractors, third party users, volunteers or trustees) of CCF are required to be aware of and follow this procedure in the event of a personal data breach; and all are responsible for reporting any personal data breach to the Data Protection Officer.

8.3 *Administrative Procedure*

The Data Protection Officer will record every data breach reported to them in a Data Security Breach Log and notify the supervisory authority and affected data subjects in accordance with the obligations set out under the UK GDPR, as summarised below.

All entries in the log will be reported to and considered by the Governance Committee, so that the Committee may take any additional remedial action that is needed.

8.3.1 *Procedure – breach notification data processor to data controller*

Each data processor appointed by CCF will report any personal data breach or security incident to CCF's Data Protection Officer, or, in their absence, the CEO, without undue delay.

The breach notification will be made by telephone, followed by e-mail giving a full description of the nature of the breach, the data affected and the individuals affected.

Cambridgeshire Community Foundation

CCF's Data Protection Officer will confirm receipt of the notification by e-mail.

8.3.2 *Procedure – breach notification data controller to supervisory authority*

In consultation with the CEO, CCF's Data Protection Officer will determine if the supervisory authority needs to be notified in the event of a breach.

If a risk to data subject(s) is likely, CCF's Data Protection Officer will report the breach to the supervisory authority, the Information Commissioner's office, without undue delay and in any event within 72 hours using the ICO's standard reporting form: <https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/>.

If it is not possible to provide all the necessary information relating to the breach at that time, CCF's Data Protection Officer will provide the information in phases without undue delay.

The following information needs to be provided to the supervisory authority (Article 33 UK GDPR):

- the nature of the personal data breach, including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer or other contact point where more information can be obtained;
- the likely consequences of the personal data breach;
- the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

CCF shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken.

8.3.3 *Procedure –breach notification data controller to data subject*

If the personal data breach is likely to result in a high risk to the rights and freedoms of the data subject, CCF will notify the data subject immediately.

If the breach affects a large number of data subjects and personal data records, CCF will make a decision based on an assessment of the effort required to notify each data subject individually and whether that effort would hinder CCF's ability to provide the notification within the specified time frame. In such circumstances, a public communication or similar measure will be used to inform those affected in an equally effective manner.

Cambridgeshire Community Foundation

9.0 Document control

The CEO is the owner of this document (as stated in the policy header) and is responsible for ensuring that this policy is reviewed in accordance with the schedule above.

Linked Policies / Statements

This policy is linked to CCF's Privacy Statement and data retention schedule