Policy Number	Name of Policy	Owned by
CCF/CEO/002	Data Protection Policy	CEO

Review Date	Reviewed by	Frequency of Review	Next Review Date
April 2021	Board 22/4/20 & Gov Comm 12/4/21	Annual	April 2022

1.0 Introduction

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

- the General Data Protection Regulation (GDPR) and any related legislation which applies in the UK, including any legislation derived from the Data Protection Bill 2017
- all other applicable laws and regulations relating to the processing of personal data and privacy, including statutory instruments and, where applicable, the guidance and codes of practice issues by the Information Commissioner's Office (ICO) or any other supervisory authority.

This policy sets out what we do to 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: 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 GDPR and with this policy is Michael O'Toole, CEO.

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.

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 other service providers which handle personal data on our behalf.

2.5 **European Economic Area (EEA)** includes all countries in the European Union as well as Norway, Iceland and Liechtenstein.

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

2.8 **Sensitive Personal Data** 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
- such other categories of personal data as may be designated as 'special categories of personal data' under the Legislation.

3.0 Data Protection Principles

Anyone processing personal data must comply with the six data protection principles set out in the GDPR. We are required to comply with these principles and show that we comply in respect of any personal data that we deal with 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 can be satisfied, including where the data subject has given consent, or where the processing is necessary for one or more specified reasons, such as where it is necessary for 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 well be collecting (categories of personal data concerned)
- that CCF will be holding their information together with 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, or 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 transferring their personal data outside the EEA and details of relevant safeguards
- 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 his or her self, 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 addition, in both scenarios (where personal data is obtained both directly and 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 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 only processed for the specific, explicit and legitimate purposes that the individual was told about when we first obtained their information. This means that we shall not collect personal data for one purpose and then use it for another. If it becomes necessary to process a person's information for a new purpose, the individual should be informed of the new purpose beforehand. For example, if we collect personal data such as a contact number or email address, in order to update a person about our activities it should not then be used for any new purpose without first getting the individual's consent.

3.3 Personal data should be adequate and accurate

The third and fourth data protection principles require that personal data that 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 personal data which is inaccurate 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 it was collected for. This means that the personal data that we hold will be destroyed or erased from our systems when it is no longer needed which is normally for a maximum of six years after our relationship with an individual has ceased; although we are occasionally required to hold data for longer periods for specific programmes.

3.5 Rights of individuals under the GDPR

The GDPR gives people rights in relation to how organisations process their personal data. Everyone who holds personal data on behalf of CCF needs to be aware of these rights. They include (but are not limited to) the right:

- 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)
- 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 prevent processing that is likely to cause unwarranted substantial damage or distress to themselves or anyone else.

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 Transferring data outside the EEA

The GDPR requires that when organisations transfer personal data outside the EEA they take steps to ensure that the data is properly protected.

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 sensitive personal data (as defined in section 2.8). Purely financial information is not technically defined as sensitive personal data by the GDPR. However, particular care will be taken when processing such data. In order to process sensitive personal data we shall obtain explicit consent from the individuals involved.

7.0 Notification

7.1 We recognise that whilst there is no obligation for us to make an annual notification to the ICO under the GDPR, we will consult with the ICO where necessary when we are carrying out 'high risk' processing.

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 that are the result of 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 her in a Data Security Breach Log and notify the supervisory authority and affected data subjects in accordance with the obligations set out under the GDPR as summarised below.

All entries on the log will be reported to and considered by the Governance Committee so that the Committee may consider any additional remedial action which needs to be taken.

8.3.1 *Procedure – breach notification data processor to data controller*
The data processor (Hyphen8/ Chater Allen/ Quickbooks) will report any personal data breach or security incident to CCF's Data Protection Officer; or, in her 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.

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 (GDPR Art 33):

- 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 high risk to the rights and freedoms of the data subject, CCF will notify the data subject immediately.

If the breach affects a high volume of data subjects and personal data records, CCF will make a decision based on an assessment of the amount of effort involved in notifying each data subject individually, and whether it will 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.

9.0 Document control

The Operations Manager is the owner of this document and is responsible for ensuring that this policy is reviewed in line with the review requirements of the GDPR.