Data Protection Policy

To be read in association with GCF's Privacy Policy (located on our website)

Introduction

Gloucestershire Community Foundation (GCF) needs to gather and use certain information about individuals.

These can include donors, fund holders, suppliers, business contacts, employees, trustees, volunteers, grant recipients and other people the foundation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the foundation's data protection standards and to comply with the law.

Why this policy exists

This data protection policy ensures GCF:

- Compiles with the General Data Projection Regulation (GDPR) and follows good practice
- Protects the rights of staff, volunteers, grant applicants, fund holders and partners
- Is open and transparent about how its stores and processes individuals' data
- Protects itself from the risks of a data breach
- Protects itself from reputational risk

Data protection law

GDPR 2018 describes how organisations – including GCF – must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

GDPR is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways
8. Not be transferred outside of the European Union (EU), unless that country or territory also ensures an adequate level of protection

Data Protection Policy

To be read in association with GCF's Privacy Policy (located on our website)

People, risks and responsibilities

Policy scope

This policy applies to:

- All GCF's offices
- All staff and volunteers including trustees and committee and panel members ('employees')
- All contractors, suppliers and other people working on behalf of GCF

It applies to all data that the foundation holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 2018. This can include:

Names of individuals

- Postal addressees
- Email address
- Telephone numbers
- … plus any other information relating to individuals

Data protection risks

This policy aims to protect GCF from some very real data security risks, including:

- **Breaches of confidentiality** – for instance, information being given out inappropriately
- **Failing to offer choice** – for instance, all individuals should be free to choose how GCF uses data relating to them as governed by the Fundraising Regulations, GDPR, PECA and the TPS.
- **Reputational damage** – for instance, GCF could suffer if hackers successfully gained access to sensitive data

Responsibilities

Everyone who works and volunteers for or with GCF has some responsibility for ensuring data is collected, stored and handled appropriately.

Each person that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, the following roles have key areas of responsibility:

The Board of Trustees is ultimately responsible for ensuring that GCF meets its legal obligations,

- The Data Protection Officer (DPO) is responsible for:
  - Keeping the Board of Trustees updated about data protection responsibilities, risks and issues, including notification of any breaches
  - Reviewing all data protection procedures and related policies
  - Arranging data protection training and advice for the people covered by this policy
  - Handling data protection questions from staff and anyone else covered by this policy
  - Dealing with requests from individuals to see the data GCF holds about them (also called 'subject access requests')
  - Checking and approving any contracts or agreements with third parties that may handle GCF's sensitive data

- The DPO is responsible for:
  - Ensuring all systems, services and equipment used for storing data meet acceptable security standards
  - Performing regular checks and scans to ensure security hardware and software is functioning properly
  - Evaluating any third-party services, the foundation is considering using to store or process data. For instance, cloud computing services, remote backup services

- The DPO is responsible for:
  - Approving any data protection statements attached to communications such as emails
  - Addressing any data protection queries from journalists or media outlets like newspapers and magazines
  - Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles

General staff guidelines

- The only people able to access data covered by this policy should be those who **need it for their work**
- Data **should not be shared informally**
- GCF will provide training to all employees to help them understand their responsibilities when handling data
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below
- **Strong passwords** must be used, and they should never be shared
- Personal data **should not be disclosed** to unauthorised people, either within GCF or externally
- Data should be **regularly reviewed and updated**. If no longer required, it should be deleted and disposed of
- Employees **should request help** from their line manager or the DPO if they are unsure about any aspects of data protection.

Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the DPO or data controller.

When data is **stored on paper**, it should be kept in a secure place where unauthorised people cannot see it.

Data Protection Policy

To be read in association with GCF's Privacy Policy (located on our website)

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- Employees and volunteers should make sure paper and printouts are **not left where unauthorised people could see them**, like on a printer or on their desk at the end of their working day (visible to cleaners/contractors)
- **Data printouts should be disposed of securely** when no longer required via the secure shredding bin
- When data is **stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts
- Data should be **protected by strong passwords** that are changed regularly and never shared between colleagues
- If data is **stored on removable media** (ie CD, DVD, memory stick), these should be kept locked away securely when not being used.
- Data should only be stored on an official GCF computer and should only be uploaded to an approved cloud computing system (Salesforce/365Sharepoint).
- Data should be **backed up frequently.** Those backups should be tested regularly
- Data should **never be saved directly** to laptops or other mobile devices like tablets or smart phones unless the mobile device is encrypted
- All servers and computers containing data should be protected by **approved security software and firewalls**
- **Laptops** used externally should only access the internet via a **secure logon**

Data use

Personal data is of no value to GCF unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees and volunteers should ensure the screens of their computers are locked when left unattended
- Personal data should not be stored on the hard drive of laptops

Data Protection Policy

To be read in association with GCF's Privacy Policy (located on our website)

Data accuracy

The law requires GCF to take all reasonable steps to ensure data is kept accurate and up to date.

It is the responsibility of all employees and volunteers who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.

Staff should take every opportunity to ensure data is updated.

GCF will make it easy for data subjects to update the information GCF holds about them

Data should be updated as inaccuracies are discovered. For instance, if a contact can no longer be reached on their stored contact number or email, it should be removed from the database.

Subject access requests

All individuals who are the subject of personal data held by GCF are entitled to:

- Ask what information the foundation holds about them and why
- Ask how to gain access to it
- Be informed how to keep it up to date
- Be informed how GCF is meeting its data protection obligations

If an individual contacts GCF requesting this information, this is called a 'subject access request'.

Subject access requests from individuals should be made by email, addressed to the DPO at info@gloucesteshirecf.org.uk. The DPO will aim to provide the relevant data within one month of the date of the request.

The DPO will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing data for other reasons

In certain circumstances, the GDPR allows personal data to be disclosed if required to do so by law without the consent of the data subject.

Under these circumstances, GCF will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the Chair and Trustees where necessary.

GCF will not share Data for any other reason than mentioned above.

Data Protection Policy

To be read in association with GCF's Privacy Policy (located on our website)

Providing information

GCF aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these lines, GCF has a privacy policy, setting out how it uses data relating to individuals. A copy of the privacy policy is available on the GCF website.

All staff and volunteers associated with GCF are required to familiarise themselves with GCF's Privacy Policy.