GDPR and Data Protection Policy

Introduction

GoCreate Taunton CIC needs to gather and use certain information about individuals in order to conduct its business. These can include students, suppliers, business contacts, employees and other people the organisation 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 company's data protection standards — and to comply with the law.

Why this policy exists

This policy ensures GoCreate Taunton CIC:

- Complies with data protection law and follows good practice
- Protects the rights of staff, customers and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Data protection law

The General Data Protection Regulation describes how organisations – including GoCreate Taunton CIC – must collect, handle and store personal information. The legislation applies regardless of whether data is stored electronically, on paper or on other materials.

Article 5 of the GDPR requires that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;
b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data are inaccurate,
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Article 5(2) requires that:

“the controller shall be responsible for, and be able to demonstrate, compliance with the principles.”

The GDPR provides the following rights for individuals:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

People, risks and responsibilities

Policy scope

This policy applies to:

- The offices of GoCreate Taunton CIC
- All staff of GoCreate Taunton CIC
- All contractors, suppliers and other people working on behalf of GoCreate Taunton CIC

It applies to all data that the company holds relating to identifiable individuals. This can include

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Date of birth
- Gender

Data protection risks

This policy helps to protect GoCreate Taunton CIC from 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 the company uses data relating to them.
- **Reputational damage.** For instance, the company could breach GDPR if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with GoCreate Taunton CIC has some responsibility for ensuring data is collected, stored and handled appropriately.

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

However, these people have key areas of responsibility:

- The **Directors** are ultimately responsible for ensuring that GoCreate Taunton CIC meets its legal obligations.
- The **Data Protection Officer** is responsible for:

o Keeping the board updated about data protection responsibilities, risks and issues.
o Reviewing all data protection procedures and related policies, in line with an agreed schedule.
o Arranging data protection training and advice for the people covered by this policy.
o Handling data protection questions from staff and anyone else covered by this policy.
o Dealing with requests from individuals to see the data GoCreate Taunton CIC holds about them ('subject access requests').
o Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
o Approving any data protection statements attached to communications such as emails and letters.
o Addressing any data protection queries from journalists or media outlets like newspapers.
o Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.
o Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
o Performing regular checks and scans to ensure security hardware and software is functioning properly.
o Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.

General staff responsibilities

- 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**.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, **strong passwords must be used** and they should never be shared.
- Personal data **should not be disclosed** to unauthorised people, either within the company or externally.
- Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of.

Data storage

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

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

- When not required, the paper or files should be kept **in a locked drawer or filing cabinet, or in a locked room**.
- Employees should make sure paper and printouts are **not left where unauthorised people could see them**, like on a printer.
- **Data printouts should be shredded** and disposed of securely when no longer required.

When data is **stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data must be **protected by strong passwords** that are changed regularly and never shared.
- If data is **stored on removable media,** these will be kept locked away securely when not being used.
- Data should only be stored on **designated drives and servers**, and should only be uploaded to **approved cloud computing services**.
- All computers containing data should be protected by **approved security software and a firewall**.

Data use

- When working with personal data, employees should ensure **the screens of their computers are always locked** when left unattended.
- Personal data **should not be shared informally**. In particular, it should never be sent by unencrypted email, as this form of communication is not secure.
- Personal data must be **encrypted before being transferred electronically**.

Data accuracy

The law requires GoCreate Taunton CIC to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort GoCreate Taunton CIC should put into ensuring its accuracy.

It is the responsibility of all employees 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 **take every opportunity to ensure data is up to date.** For instance, by updating address' should someone move.

- Data should be **updated as inaccuracies are discovered**. For instance, if someone can no longer be reached on their stored telephone number, it should be removed.

Information requests

All individuals who are the subject of personal data held by GoCreate Taunton CIC are entitled to:

- Confirmation that their personal data is being processed and why
- Ask what information the company holds about them and why including
  - The categories of personal data involved
  - Who the information has been, or will be, disclosed to
  - The length of time the data will be held for
  - Who provided the information (if not the individual themselves)
  - Whether their data is involved in automated decision-making such as profiling
  - Ask how to gain access to personal data
- Be informed on how to keep personal data held up to date
- Be informed on how GoCreate Taunton CIC is meeting its data protection obligations including access to GoCreate Taunton CIC's Privacy Notice

If an individual contacts the company requesting this information, this is called a subject access request.

Subject access requests should be made by email. Emails received in relation to an Information Request will be held once the enquiry has been satisfied in order to track repeat or nuisance requests, which may incur an administrative charge.

In all cases, it is essential that the identity of the person requesting the information must be verified by reasonable means before any personal data is shared.

Disclosing data for other reasons

In certain circumstances, the General Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, GoCreate Taunton CIC will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

Privacy Notice

GoCreate Taunton CIC 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