# Shared Future CIC

# Data Protection Policy Statement

## 1. Policy statement

You must read this policy because it gives important information about:

a. the data protection principles with which Shared Future CIC (SFCIC) must comply;

b. what is meant by personal data (or data) and sensitive personal data (or data);

c. how we gather, use and (ultimately) delete personal data and sensitive personal data in accordance with the data protection principles;

d. where more detailed privacy information can be found about the personal data we gather and use, how it is used, stored and transferred, for what purposes, the steps taken to keep that information secure and for how long it is kept;

e. the individuals' rights and obligations in relation to data protection; and

f. the consequences of failure to comply with this policy.

## 2. Aims of this policy

SFCIC needs to keep certain information on its Directors, Associates, Clients and Beneficiaries, to carry out its day to day operations, to meet its objectives and to comply with legal obligations.

Shared Future CIC is committed to processing data in accordance with its responsibilities under the GDPR.

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; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial 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 that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

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.

## 3. Scope

a. This policy applies to all personal data processed by Shared Future CIC

b. The Responsible Person shall take responsibility for Shared Future CIC's ongoing compliance with this policy.

c. This policy shall be reviewed at least annually.

d. Shared Future CIC shall register with the Information Commissioner's Office as an organisation that processes personal data.

e. Everyone managing and handling personally identifiable information is trained to do so.

f. Anyone wanting to make enquiries about handling personal identifiable information, whether a member of staff, volunteer or otherwise, knows what to do;

g. Any disclosure of personal data will be in line with our procedures.

h. Queries about handling personal information will be dealt with swiftly and politely.

## 4. Definitions

| | |
|---|---|
| **data breach** | means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data; |
| **data subject** | means the individual to whom the personal data relates; |
| **personal data** | (sometimes known as personal data) means data relating to an individual who can be identified (directly or indirectly) from that data; |
| **processing data** | means obtaining, recording, organising, storing, amending, retrieving, disclosing and/or destroying data, or using or doing anything with it; |
| **sensitive personal data** | (sometimes known as 'special categories of personal data' or 'sensitive personal data') means personal data about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetics information, biometric information (where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation |

## 5.Data protection principles

a. **Lawful, fair and transparent processing:**

   a. To ensure its processing of data is lawful, fair and transparent, Shared Future CIC shall maintain a Register of Systems.

   ii. The Register of Systems shall be reviewed at least annually.

   iii. Individuals have the right to access their personal data and any such requests made to Shared Future CIC shall be dealt with in a timely manner.

b. **Lawful purposes**

   i. All data processed by Shared Future CIC must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests (see ICO guidance for more information).

   ii. Shared Future CIC shall note the appropriate lawful basis in the Register of Systems.

   iii. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.

   iv. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in the SFCIC's systems.

c. **Data minimisation**

   i. Shared Future CIC shall ensure that personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

d. **Accuracy**

   i. Shared Future CIC shall take reasonable steps to ensure personal data is accurate.

   ii. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

e. **Archiving / removal**

   i. To ensure that personal data is kept for no longer than necessary, Shared Future CIC shall put in place an archiving policy for each area in which personal data is processed and review this process annually.

   ii. The archiving policy shall consider what data should/must be retained, for how long, and why.

f. **Security**

   i. Shared Future CIC shall ensure that personal data is stored securely using modern software that is kept-up-to-date.

   ii. Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.

   iii. When personal data is deleted, this should be done safely such that the data is irrecoverable.

   iv. Appropriate back-up and disaster recovery solutions shall be in place.

## 6. Sensitive personal data

a. Sensitive personal data is sometimes referred to as 'special categories of personal data' or 'sensitive personal data'.

b. We may from time to time need to process sensitive personal data. We will only process sensitive personal data if:

   i. we have a lawful basis for doing so;

   ii. one of the special conditions for processing sensitive personal data applies, including:

      - the data subject has given has given explicit consent;
      - the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent;

- processing relates to personal data which are manifestly made public by the data subject
- the processing is necessary for the establishment, exercise or defence of legal claims;
- the processing is necessary for reasons of substantial public interest.

c. Sensitive personal data will not be processed until the individual has been properly informed (by way of a privacy notice or otherwise) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

d. Shared Future CIC will not carry out automated decision-making (including profiling) based on any individual's sensitive personal data.

e. Shared Future CIC's data privacy notices internally, for employees and associates; and externally, for members, set out the types of sensitive personal data that SFCIC processes, what it is used for and the lawful basis for the processing.

## 7.Data protection impact assessments (DPIA)

a. Where processing is likely to result in a high risk to an individual's data protection rights (for example, where the SFCIC is planning to use a new form of technology), we will, before commencing the processing, carry out a DPIA to assess:

   i. whether the processing is necessary and proportionate in relation to its purpose;

   ii. the risks to individuals; and

   iii. what measures can be put in place to address those risks and protect personal data.

b. Before any new form of technology is introduced, the manager responsible should review the guidance available on conducting a DPIA and contact the Compliance Function for advice in carrying out as assessment.

## 8. Documentation and records

a. We will keep written records of processing activities, primarily in SFCIC's Data Processing register, including but not limited to:

   i. the purposes of the processing;

   ii. a description of the categories of individuals and categories of personal data;

b. categories of recipients of personal data;

c. where possible, retention schedules; and

d. where possible, a description of technical and organisational security measures; and

e. the lawful basis for our processing.

## 9. Individual rights

a. All data subjects have the following rights in relation to their personal data:

   i. to be informed about how, why and on what basis that data is processed—see the SFCIC's Data Protection Privacy notices;

ii. to obtain confirmation that your data is being processed and to obtain access to it and certain other data, by making a subject access request;

iii. to have data corrected if it is inaccurate or incomplete;

iv. to have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing (this is sometimes known as 'the right to be forgotten');

v. to restrict the processing of personal data where the accuracy of the data is contested, or the processing is unlawful (but you do not want the data to be erased), or where the employer no longer needs the personal data but you require the data to establish, exercise or defend a legal claim; and

vi. to restrict the processing of personal data temporarily where you do not think it is accurate (and the employer is verifying whether it is accurate), or where you have objected to the processing (and the employer is considering whether the organisation's legitimate grounds override your interests).

b. Employees wishing to exercise any of the rights in paragraph 9(a), please contact Jayne McFadyen.

c. Subject access requests: anyone whose personally identifiable information we process has the right to know:

i. What information we hold and process on them

ii. How to gain access to this information

iii. How to keep it up to date

iv. What we are doing to comply with the Act.

In some circumstances they have the right to prevent processing of their personally identifiable information and the right to correct, rectify, block or erase personally identifiable information regarded as wrong.

Any person wishing to exercise this right should apply in writing to Shared Future CIC at our registered office.

## 10. Individual obligations

a. Individuals are responsible for helping SFCIC keep their personal data up to date. You should let our HR director know if the data you have provided to SFCIC changes, for example if you move house or change details of the bank or building society account to which you are paid.

b. You may have access to the personal data of other members of staff, associates and, clients of SFCIC in the course of your employment. SFCIC expects you to help meet its data protection obligations to those individuals.

c. If you have access to personal data, you must:

i. only access the personal data that you have authority to access, and only for authorised purposes;

ii. only allow other SFCIC staff to access personal data if they have appropriate authorisation;

iii. keep personal data secure by complying with rules on access to premises, computer access, password protection and secure file storage and destruction and other precautions set out in SFCIC's information security policy;

iv. not store personal data on local drives or on personal devices that are used for work purposes.

d. You should contact Jayne McFadyen if you are concerned or suspect that one of the following has taken place (or is taking place or likely to take place):

i. processing of personal data without a lawful basis for its processing or, in the case of sensitive personal data, without one of the conditions in paragraph 6 being met;

ii. any data breach as set out in paragraph 13 below; access to personal data without the proper authorisation; or personal data not kept or deleted securely;

iii. any other breach of this policy or of any of the data protection principles set out in paragraph 5 above.

## 11. Information security

a. SFCIC will use appropriate technical and organisational measures in accordance with SFCIC's Information Security Policy to keep personal data secure, and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage. These may include:

i. making sure that, where possible, personal data is pseudonymised or encrypted;

ii. ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

iii. ensuring that, in the event of a physical or technical incident, availability and access to personal data can be restored in a timely manner; and

iv. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

b. Where SFCIC uses external organisations to process personal data on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal data. In particular, contracts with external organisations must provide that:

i. the organisation may act only on the written instructions of SFCIC;

ii. those processing the data are subject to a duty of confidence;

iii. appropriate measures are taken to ensure the security of processing;

iv. sub-contractors are only engaged with the prior consent of SFCIC and under a written contract;

v. the organisation will assist SFCIC in providing subject access and allowing individuals to exercise their rights in relation to data protection;

vi. the organisation will assist SFCIC in meeting its obligations in relation to the security of processing, the notification of data breaches and data protection impact assessments;

vii. the organisation will delete or return all personal data to SFCIC as requested at the end of the contract; and

viii. The organisation will submit to audits and inspections, provide SFCIC with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell SFCIC immediately if it is asked to do something infringing data protection law.

c. Before any new agreement involving the processing of personal data by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval of its terms by the relevant Director.

## 12. Storage and retention of personal data

a. Personal data (and sensitive personal data) will be kept securely in accordance with SFCIC's Information Security Policy.

b. Personal data (and sensitive personal data) should not be retained for any longer than necessary. The length of time over which data should be retained will depend upon the circumstances, including the reasons why the personal data was obtained. Where there is any uncertainty, staff should consult the Compliance Function.

c. Personal data (and sensitive personal data) that is no longer required will be deleted permanently from our information systems and any hard copies will be destroyed securely.

## 13. Data Breach

a. A data breach may take many different forms, for example:

   i. loss or theft of data or equipment on which personal data is stored;

   ii. unauthorised access to or use of personal data either by a member of staff or third party;

   iii. loss of data resulting from an equipment or systems (including hardware and software) failure;

   iv. human error, such as accidental deletion or alteration of data;

   v. unforeseen circumstances, such as a fire or flood;

   vi. deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and

   vii. obtaining data by deceiving the organisation which holds it.

b. In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, SFCIC shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO (more information on the ICO website).

c. We will notify the affected individuals if a data breach is likely to result in a high risk to their rights and freedoms.

## 14. Training

a. We will ensure that:

   i. Training and awareness raising about the Data Protection Act and how it is followed in this organisation will take the following forms:

   ii. On induction: all new Directors, associates, employed staff and volunteers will be informed of SFCIC's data protection policies and of their individual responsibilities when processing, handling and storing data.

## 15. Reviewing this policy

As an organization, it is SFCIC's policy to review and revise this policy as necessary at regular intervals and inform Directors, associates, employed staff and volunteers of any changes.

This policy will be reviewed at intervals of two years to ensure it remains up to date and compliant with the law.

| | |
|---|---|
| *(Responsible Director)* | Jayne McFadyen |
| *(Named Project Lead)* | has responsibility for ensuring this policy is put into practice on location during projects and events. |

**Review history**

| *Review Date* | *Reviewer* |
|---|---|
| 4th June, 2020 | Jayne McFadyen |
| 27th January, 2022 | Alex King |
| 22nd April 2024 | Jez Hall |