

Data Protection Policy

Version 4

01/05/2026

Document Control

Status	Signed off by Board	Version	4.00
Location			

Version Control

Revision Date	Amendment	Issued By	Approved By	New Version No.
February 2023	Adapted from FareShare Midlands policy here: https://faresharemidlands.org.uk/data-protection/	Susy Salino	Board and SLT	2.00
March 2023	Adapted in line with recommendations from SLT	Susy Salino	Board and SLT	3.00
May 2026	Combined handbook data protection with this policy. Added name change of national partner charity. Added changes in line with DUAA new regulations	Catherine Naughton and Susie Day	Board and SLT	4.00

Distribution List

Version No.	Issued to (Name)	Date of Issue
4.00	All Staff	06/08/2026


Signed

Role Deputy Chief Executive Officer

Contents

Data Protection Policy.....	1
Policy Statement	3
Purpose and scope	4
Principles	4
Procedures.....	5
Internal data records.....	5
Purposes.....	5
Disclosure and Barring Service.....	6
Access.....	6
External data records.....	7
Purposes.....	7
Access.....	7
Storage	7
Data Subject Access Request (DSAR) procedure.....	8
DSAR complaints procedure	9
Accuracy	9
Storage	9
Use of Photographs and Film.....	9
Procedures.....	9
Responsibilities of staff, volunteers, and trustees	9
Compliance.....	9
Breach of data Security.....	10
Retention of Data.....	10
Destruction of personal data.....	10

Policy Statement

Community Initiatives South West Ltd (registered name, referred to as FareShare South West from here on) collects and uses information about people with whom it communicates. This personal information must be dealt with properly and securely however it is collected, recorded, and used - whether on paper, in a computer, or recorded on other material - and there are safeguards to ensure this in the Data

Protection Act 2018 and the Data Use and Access Act 2025 (DUAA). FareShare South West fully endorses and adheres to the Principles of Data Protection, as set out in the Data Protection Act 2018 and the General Data Protection Regulations (GDPR).

Purpose and scope

The purpose of this policy is to ensure that the staff, volunteers and trustees, members, contractors, consultants, donors, supporters, and all other and service users of FareShare South West are clear about the purpose and principles of Data Protection and to ensure that we have guidelines and procedures in place which are consistently followed.

Failure to adhere to the Data Protection Act 2018, the DUAA and UK GDPR is unlawful and could result in legal action being taken against FareShare South West or its staff, volunteers, or trustees.

Definitions for this policy

Who you're talking to

'FareShare South West' is a trading name of Community Initiatives South West Limited; Company number 6130395, registered charity number 1125905, registered address Unit 4 Little Ann Street, St Judes, Bristol, BS2 9EB.

In this policy, any reference to "we" or "us" refers to FareShare South West.

'Felix' refers to the charity entity Felix, which recently merged the national charity FareShare with The Felix Project. FareShare South West is an independent charity which works in partnership with Felix. Felix provide FareShare South West with data management software in order to support our service. Your data may be held by both FareShare South West and Felix as a result.

This Data Protection Policy relates only to data held by FareShare South West. For information about Felix's handling of your data, please refer to Felix's Data Protection Policy.

Personal Data

Personal Data means data about a living individual who can be identified from those data (or from those and other information either in our possession or likely to come into our possession). Special category data is personal data which needs more protection because it is sensitive. Non-personal data means data that is in no way personally identifiable.

Principles

The Data Protection Act 2018 regulates the processing of information relating to living and identifiable individuals (data subjects). This includes the obtaining, holding, using, or disclosing of such information, and covers computerised records as well as manual filing systems and card indexes.

Any staff member, volunteer or trustee who collects, stores, accesses or analyses personal data at FareShare South West (FSSW) is a data user. We ensure that all comply with the data protection principles of good practice which underpin the Act and collect and use

information fairly, lawfully, and transparently. We follow the key principles of GDPR, which are summarised below:

1. Lawfulness, fairness, and transparency
2. Purpose limitation
3. Data minimisation
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality (security)
7. Accountability

The principles apply to personal data which is defined as [‘any information which is related to an identified or identifiable natural person’](#). FareShare South West’s employees, volunteers and trustees who process or use any personal information in the course of their duties will ensure that these principles are followed at all times.

The DUAA upholds these principles, while clarifying legitimate interest and making provisions specific to charity communications. The DUAA is being implemented in phases in 2025 and 2026. This policy will indicate whenever the Act is relevant.

Procedures

The following procedures have been developed in order to ensure that FareShare South West meets its responsibilities in terms of Data Protection. For the purposes of these procedures data collected, stored, and used by FareShare South West falls into 2 broad categories: -

- FareShare South West internal data records; staff, volunteers, and trustees
- FareShare South West externally hosted data records; members, volunteers, employability participants, partner organisations, food suppliers, donors, and supporters

FareShare South West as a body is a data controller under the Act, and the Senior Leadership Team is ultimately responsible for the policy’s implementation, with the CEO acting as Data Protection Officer (DPO).

Please refer to the Privacy Policy for further information about how your data is processed.

Internal data records

Purposes

FareShare South West obtains personal data (names, addresses, phone numbers, email addresses), application forms, and references and in some cases other documents from staff, volunteers, and trustees.

Employed staff:

When you sign a contract of employment with FareShare South West, you consent to the processing of such data both inside and, where necessary, outside the European Economic Area for the purposes of:

- salary, benefits and pensions administration and employee management
- health administration and for the purposes of health insurance/benefits
- training and appraisal, including performance records and disciplinary records
- equal opportunities monitoring
- any potential change of control of FSSW or any potential transfer of your employment under the Transfer of Undertakings (Protection of Employment) Regulations 2006 (as amended). In such circumstances, disclosure may include disclosure to the potential purchaser or investor and their advisors
- promoting or marketing of FSSW or its products or services
- compliance with applicable procedures, laws and regulations
- any other reasonable purposes in connection with your employment, about which you shall be notified from time to time

In order to fulfil the purposes set out above, it may be necessary to pass your personal data (or special category personal data, as appropriate) to regulatory bodies, government agencies and other third parties as required by law or for administration purposes.

Staff agree to use all reasonable endeavours to keep FSSW informed of any changes to their personal data or sensitive personal data and to comply with all relevant data protection legislation.

FareShare South West may be required to process personal data or special category personal data about you if you are a volunteer or trustee. This data will only be processed for:

- equal opportunities monitoring (anonymised)
- supporting your health, for example providing reasonable adjustments
- complying with DBS requirements when the role requires it
- compliance with applicable procedures, laws and regulations

Disclosure and Barring Service

FareShare South West will act in accordance with the DBS code of practice. Only Certificate numbers of any DBS checks will be held by FareShare South West in HR records, in line with the timelines in the HR Data Privacy Notice and Retention of Records schedule.

Access

FareShare South West uses a personnel system (Breathe HR) for data on employees. It records employment details and personal contact details. All employees have access to this system and can view their own personal data and that of the people they line manage. It is the responsibility of the individual employee to update these if personal details change (such as home address or emergency contact details). Only the CEO, Deputy CEO and HR & Finance Assistant have universal access to employee data.

Volunteer personal data (name, date of birth, email address, home address) is stored on a volunteer management system owned by the national charity Felix. Volunteer personal data is also securely stored in a supporter management system by FareShare South West. Both organisations have a responsibility to uphold the principles of the Data Protection Act 2018, UK GDPR and DUAA in processing this data. Felix have a separate Data Protection Policy to refer to. Please refer to the FareShare South West privacy policy for further information about how we process your data.

The contact details of staff, volunteers and trustees will only be made available to other staff, volunteers, and trustees on an officially verified request/ “in the line of duty” basis. Any other information supplied on application will be kept in secure Electronic Folders or filing cabinet and is not accessed during the day to day running of the organisation, except as needed for recruitment or operational purposes.

Contact details of staff, volunteers and trustees will not be passed on to anyone outside the organisation without their explicit consent and where officially verified as necessary by the CEO or Deputy CEO in the CEO’s absence. HR advice will be sought in case of any issues of doubt and/or concern.

Staff, volunteers, and trustees will be supplied with a copy of their personal data held by the organisation if a request is made.

All confidential post must be opened by the addressee only.

External data records

Purposes

FareShare South West obtains personal data and information from clients and members in order to provide services and communicate relevant information. These data are stored and processed only for purposes of legitimate interest and can be opted out of at any time.

Access

Only the organisation’s relevant staff, volunteers and trustees will normally have access to personal data. All staff, volunteers and trustees are made aware of the Data Protection Policy and General Data Protection Regulation (GDPR) and their obligation not to disclose personal data to anyone who is not supposed to have it. All staff with access to personal data undergo internal training relating to the safe collection and handling of personal data. Information supplied is kept in a secure filing, paper and electronic system and is only accessed by those individuals involved in the delivery of the service. Information will not be passed on to anyone outside the organisation without their explicit consent, excluding statutory bodies e.g., the Inland Revenue.

All confidential post must be opened by the addressee only unless the staff member has left the organisation.

Storage

Personal data may be kept in paper-based systems and on a password-protected computer system. Paper-based data are stored securely in locked office spaces.

We may employ third party companies and individuals to facilitate our Service, to provide the Service on our behalf, to perform Service-related services or to assist us in analysing how our Service is used. These third parties have access to your Personal Data only to perform these tasks on our behalf and are obligated not to disclose or use it for any other purpose.

Personal data will be stored for as long as the data owner/ client/ member uses our services and normally longer in line with statutory requirements. Where an individual ceases to use our services and it is not deemed appropriate to keep their records, their records will be destroyed. However, unless we are specifically asked by an individual to destroy their details, we will keep them on file for future reference. If a request is received from an organisation/ individual to destroy their records, we will remove their details from the database and request that all staff holding paper or electronic details for the organisation destroy them.

This procedure applies if FareShare South West is informed that an organisation ceases to exist.

Data Subject Access Request (DSAR) procedure

By law, people have a right to access and a copy of any information FareShare South West stores that uses their personal data through a DSAR. The DUAA clarifies that the organisation is required to undertake reasonable and proportionate action to fulfil its obligations, for example focusing on where data is most likely to be held.

On receiving a DSAR, FareShare South West's data protection officer will take these steps:

1. Check that the requester is who they say they are. If the DSAR is made on behalf of the data subject e.g., a solicitor or relative, the DPO will ask for written authority to act on behalf of the person concerned. This includes parents or carers of children aged 12 and over.
2. Work with the Senior Leadership Team to take reasonable and proportionate action to gather data relating to the data subject within one calendar month of receiving confirmation on the checks. This includes electronic and paper files. If the DSAR's due date falls on a weekend, then the DPO has until the next working day to respond. If it is a multiple or very complex request, the DPO will alert the requester that it will take up to three months. The DUAA incorporates a 'stop the clock' principle: if further information from the requester is required to clarify the scope of their request or to verify their identity, this response period will be paused, providing the requester is informed promptly. The time taken to obtain clarification /verification does not count toward the mandated timeframe.
3. Double check the information to ensure that it only lists the requester's personal data. Any information that doesn't relate to the person making the DSAR will be redacted unless FareShare South West has consent from other data subjects to share their data with the requester.
4. Reply by email unless the requester has said otherwise, checking with them what format they'd like it sent and ensuring it is sent securely, along with a copy of our privacy policy.
5. Store a record of what has been sent in a secure place.

DSAR complaints procedure

If the requester wishes to make a complaint about the handling of their DSAR, they should complete the complaints form on the FSSW website. On receipt, the FareShare South West data protection officer will:

1. Acknowledge the complaint within 30 days
2. Take appropriate steps to investigate and respond without undue delay
3. Keep complainants informed of progress and outcomes

Accuracy

FareShare South West will take reasonable steps to keep personal data up to date and accurate. Personal data will be stored for up to 7 years (in line with HMRC and Accounting Standards guidance) after an employee, volunteer or trustee has worked for the organisation and brief details for longer.

Storage

Personal data are kept in paper-based systems and on a password-protected computer system. Paper-based data are stored securely in locked office spaces.

Use of Photographs and Film

Where a person is recognisable, FareShare South West will always seek written consent from individuals before displaying or sharing photographs or recorded footage in which they appear. If consent is withdrawn, we will remove any photograph or recorded footage in which that person is featured. This policy also applies to photographs published on the organisation's website and all other digital and print marketing activity. Where a partner organisation (such a Felix) requests use of these materials, additional consent will be required.

This consent is typically expected to last for 3 years if an individual does not withdraw it.

Procedures

Responsibilities of staff, volunteers, and trustees

During the course of their duties with FareShare South West, staff, volunteers, and trustees will be dealing with information such as names/addresses/phone numbers/e-mail addresses of members/clients/volunteers, for legitimate business purpose only. If an employee, volunteer, or trustee gains access to confidential information they should not have (for example overhearing a conversation), they are obliged to report this to their line manager or a member of staff, and for it to be handled as a data breach.

To ensure staff, volunteers and trustees meet the terms of the Data Protection Act, they are required to confirm they have read and understood this policy as part of their employment contract or induction. The Privacy Policy which supports the Data Protection Policy is publicly available on the FareShare South West website: [Privacy Policy - FareShare South West](#)

Compliance

Compliance with the Data Protection Act is the responsibility of all staff, volunteers, and trustees. FareShare South West will regard any unlawful breach of any provision of the Act

as a serious matter which will result in disciplinary action. Any employee who breaches this policy statement will be dealt with under the disciplinary procedure which may result in dismissal for gross misconduct. Any such breach could also lead to criminal prosecution.

Any questions or concerns about the interpretation or operation of this policy statement should, in the first instance, be referred to the individual's line manager or volunteer manager. Trustees should refer to the CEO.

Breach of data Security

If FareShare South West discovers that there has been a breach of HR-related personal data that poses a risk to the rights and freedoms of an individual(s), it will report it to the Information Commissioner within 72 hours of discovery. FareShare South West will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of an individual(s), it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

Retention of Data

No documents will be stored for longer than 7 years unless with explicit consent or for reasonable business purposes.

Destruction of personal data

All records containing personal data will be destroyed in a lawful manner within the time frames outlined above in this document. Paper records will be cross-shredded and digital records will be deleted from computers and servers. Where data is hosted externally (for example in a content management system), the host will be instructed to remove the data securely.

If you have any queries about this policy, please contact us at:

- Unit 4, Little Ann St, Bristol BS2 9EB
- info@faresharesouthwest.org.uk
- 0117 954 2220