DATA PROTECTION, DATA USE AND ACCESS POLICY

Ferryside Social Enterprise Group / Calon y Fferi Community Centre

Effective Date: June 2026

Policy Owner: Centre Managers (Data Protection Lead).
The Centre Managers act jointly as the organisation's Data Protection Leads and are responsible for day-to-day data protection compliance.

Approved By: Board of Trustees

Review Cycle: Annually or sooner if legislation, ICO guidance, or organisational activities change.

1. Purpose

Ferryside Social Enterprise Group / Calon y Fferi Community Centre is committed to protecting the privacy and personal data of everyone who engages with our services.

This policy explains how we collect, use, store, share and protect personal information in accordance with:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Data (Use and Access) Act 2025
- Relevant Information Commissioner's Office (ICO) guidance

The organisation recognises that personal data is a valuable asset that must be handled lawfully, fairly, transparently and securely.

The Centre operates primarily as a community venue and activity hub and does not routinely collect special category or safeguarding information from members of the public, except where necessary for accessibility, health and safety, safeguarding, legal obligations or the protection of individuals.

2. Scope

This policy applies to:

- Trustees
- Employees
- Volunteers
- Contractors
- Consultants
- Partner organisations processing data on our behalf

The policy applies to all personal data held in:

- Electronic systems
- Cloud services
- Paper records
- Emails
- Photographs and digital media
- CCTV systems (where applicable)

It covers information relating to:

- Service users
- Community members
- Children and young people
- Vulnerable adults
- Volunteers
- Employees
- Trustees
- Donors
- Funders
- Suppliers
- Visitors

3. Data Protection Principles

The organisation will comply with the principles set out in Article 5 UK GDPR.

Personal data shall be:

Lawful, Fair and Transparent

Collected and used in ways individuals would reasonably expect and clearly explained through privacy notices.

Purpose Limited

Collected only for specified, explicit and legitimate purposes.

Data Minimised

Limited to information that is relevant and necessary.

Accurate

Kept accurate and up to date where appropriate.

Storage Limited

Retained only for as long as necessary and in accordance with the organisation's Retention Schedule.

Secure

Protected against unauthorised access, loss, destruction, damage or disclosure.

Accountable

The organisation will be able to demonstrate compliance with data protection requirements.

4. Lawful Basis for Processing

The organisation will only process personal data where a lawful basis exists.

These may include:

Consent

For example:

- Marketing communications
- Newsletters
- Use of photographs
- Optional surveys

Contract

For example:

- Room bookings
- Event registrations
- Employment contracts
- Supplier arrangements

Legal Obligation

For example:

- Employment records
- Financial reporting
- Safeguarding obligations

- Health and safety requirements

Vital Interests

Where processing is necessary to protect someone's life or physical safety.

Legitimate Interests

For the effective management and operation of the community centre, provided those interests do not override the rights and freedoms of individuals.

5. Special Category Data

The organisation may process special category data including:

- Health information
- Disability or accessibility requirements
- Ethnicity information where required for monitoring or funding purposes
- Safeguarding information

Such data will only be processed where:

- An appropriate lawful basis exists; and
- A valid Article 9 condition under UK GDPR applies; and
- Appropriate safeguards are implemented.

Access to special category data will be restricted to authorised individuals.

6. Personal Data We Collect

Depending on the service provided, we may collect:

- Name
- Address
- Email address
- Telephone number
- Emergency contact details
- Date of birth (where relevant)
- Attendance records
- Booking information
- Volunteer records

- Employment records
- Donation records
- Health and accessibility information
- Safeguarding information
- Images and photographs
- CCTV footage (where applicable)

We will only collect information necessary for identified purposes.

7. How We Use Personal Data

We may use personal data to:

- Deliver community services and activities
- Manage bookings and events
- Support safeguarding responsibilities
- Communicate with service users and supporters
- Recruit and manage staff and volunteers
- Administer grants and funding requirements
- Maintain financial records
- Meet legal obligations
- Improve and evaluate services
- Protect the health, safety and wellbeing of individuals

The organisation will not sell personal data or use it for commercial exploitation.

8. Data Sharing and Access

8.1 Controlled Data Sharing

Information may be shared where lawful and necessary with:

- Local authorities
- Funding bodies
- Regulators
- Emergency services

- Safeguarding agencies
- Professional advisers
- Partner organisations delivering services jointly with the centre

All data sharing will:

- Have a lawful basis
- Be proportionate and necessary
- Be limited to relevant information
- Be appropriately documented
- Comply with confidentiality requirements

Where appropriate, Data Sharing Agreements will be used.

8.2 Data Processors

The organisation may use third-party service providers to process data on its behalf.

Examples include:

- Cloud storage providers
- Email services
- Accounting software
- Booking systems
- Website providers
- Payroll providers

Appropriate contracts and safeguards will be in place to ensure compliance with data protection law.

8.3 International Transfers

Where personal data is transferred outside the United Kingdom, the organisation will ensure that appropriate safeguards are in place in accordance with UK GDPR requirements.

9. Individual Rights

Individuals have the right to:

- Be informed about how their data is used
- Access their personal data

- Request correction of inaccurate data
- Request erasure where applicable
- Restrict processing
- Object to processing
- Request data portability where applicable
- Withdraw consent where consent is relied upon

Requests should be made to the Data Protection Lead.

Requests will normally be responded to within one calendar month.

10. Complaints

Individuals who have concerns regarding how their personal data has been handled should contact the Data Protection Lead in the first instance.

Complaints will be investigated promptly and fairly.

If an individual remains dissatisfied, they have the right to complain to the Information Commissioner's Office (ICO).

11. Data Retention

Personal data will be retained only for as long as necessary for the purpose for which it was collected.

Retention periods are set out in the organisation's separate Data Retention Schedule.

When information is no longer required it will be securely deleted, destroyed or anonymised.

12. Data Security

The organisation will take appropriate technical and organisational measures to protect personal data.

These measures include:

- Password-protected systems
- Multi-factor authentication where available
- Access controls based on need-to-know principles
- Secure cloud storage
- Encryption of portable devices where possible
- Secure disposal of confidential information

- Locked storage for paper records
- Regular software updates and antivirus protection
- Periodic review of user access permissions
- Staff and volunteer training

Trustees, staff and volunteers must ensure personal data is not accessed, disclosed or shared without authorisation.

13. Data Breaches

A personal data breach includes accidental or unlawful:

- Loss
- Destruction
- Alteration
- Unauthorised disclosure
- Unauthorised access

All actual or suspected breaches must be reported immediately to the Centre Manager/Data Protection Lead.

The organisation will:

1. Contain and assess the breach.
2. Record the incident.
3. Investigate causes and impacts.
4. Notify the ICO where legally required and normally within 72 hours of becoming aware of the breach.
5. Notify affected individuals where there is a high risk to their rights and freedoms.
6. Take steps to prevent recurrence.

A breach register will be maintained.

14. Roles and Responsibilities

Board of Trustees

Trustees have overall accountability for data protection governance and compliance.

Trustees will:

- Approve and review policies
- Monitor significant data protection risks
- Review serious incidents and breaches
- Ensure adequate resources and training are available
- Receive periodic reports on compliance activities

Centre Manager (Data Protection Lead)

The Centre Manager acts as the organisation's Data Protection Lead and is responsible for:

- Day-to-day compliance
- Handling data protection requests
- Managing data breaches
- Maintaining records and procedures
- Coordinating staff training
- Liaising with regulators where required

Staff and Volunteers

All staff and volunteers must:

- Follow this policy
- Maintain confidentiality
- Access only information necessary for their role
- Report concerns and breaches promptly
- Complete required training

Failure to comply may result in disciplinary or other appropriate action.

15. Training and Awareness

The organisation will ensure that all trustees, staff and volunteers receive appropriate training and guidance relevant to their responsibilities.

Training may include:

- Data protection principles
- Confidentiality

- Safeguarding information handling
- Data breach reporting
- Cybersecurity awareness

Training records will be maintained.

16. Privacy Notices

The organisation will provide clear and accessible privacy notices explaining:

- What personal data is collected
- Why it is collected
- How it is used
- How long it is retained
- Who it may be shared with
- Individual rights

Privacy notices will be available:

- At the point of data collection
- On the organisation's website (where applicable)
- Upon request

17. Monitoring and Review

This policy will be:

- Reviewed annually
- Updated following legislative or regulatory changes
- Reviewed following significant incidents or breaches
- Approved by the Board of Trustees

The Board will receive an annual data protection report covering:

- Subject access requests
- Complaints
- Data breaches
- Training completion

- Emerging risks
- Compliance actions undertaken

18. Contact Details

Data Protection Lead

Centre Managers (Job Share): Julia Amsbury or Simone Bizzell-Browning

Ferryside Social Enterprise Group / Calon y Fferi Community Centre

Email: manager@calonyfferi.org

Telephone: 01267 874040

Postal Address: Canolfan Gymunedol Calon y Fferi Community Centre, Carmarthen Road,

Ferryside, SA17 5TE

For information about data protection rights, individuals may also contact the Information Commissioner's Office (ICO)

Recoverable Signature

X James Greenwell

James Greenwell
Chair of trustee board Ferryside Social Enterp...
Signed by: 01db58a2-a457-4abe-b4b9-0e504df2ea73

Date policy reviewed: 17th of June 2026

Date that next review is due: June 2027