The Roots Foundation Wales
GDPR POLICY
V2 issue December 25

Revision History
We may update this policy from time to time. We will update the "Effective Date" on the first page of this policy to reflect the effective date of any changes to this policy.

Effective date January 2026

Introduction

The Roots Foundation Wales needs to gather and use certain information about individuals.

These can include customers, suppliers, business contacts, employees, young people, and other people the organisation has a relationship with or may need to contact.

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

Why this policy exists.
The data protection policy ensures the Roots Foundation Wales:

- Complies with data protection law and follows good practice.
- Protects the right of staff, Young People, 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 UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 set out the legal framework governing how organisations, including The Roots Foundation Wales, must collect, handle, and store personal information.
These requirements apply to all personal data held by the organisation, whether stored electronically, on paper, or in any other format.
To comply with data protection law, personal information must be:

- Collected and processed lawfully, fairly, and transparently.
- Used only for specific, explicit, and legitimate purposes.
- Adequate, relevant, and limited to what is necessary.
- Accurate and kept up to date
- Stored securely and retained only for as long as necessary.
- Managed in a way that ensures appropriate security, including protection against unauthorised or unlawful processing, accidental loss, destruction, or damage.

The Roots Foundation Wales must also ensure that personal information is not disclosed inappropriately or unlawfully, and that individuals’ data protection rights are respected at all times.

Policy scope

This policy applies to:

- The head office of the Roots Foundation Wales
- All branches of the Roots Foundation Wales
- All staff and volunteers of the Roots Foundation Wales
- All contractors, suppliers, young people, and other people working on behalf of the Roots Foundation Wales

It applies to all data that the organisation holds relating to identifiable individuals, even if that information technically falls outside of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. This can include:

- Names of individuals
- Postal addresses
- Email addresses

- Telephone numbers
- Plus, any other information relating to individuals.

Data protection risks

This policy helps to protect the Roots Foundation Wales 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 the organisation uses data relating to them.
- Reputational damage – for instance, the organisation could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with the Roots Foundation Wales has responsibility for ensuring data is collected, stored, and managed appropriately.
Each team that manages personal data must ensure that it is managed and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- The board of directors is ultimately responsible for ensuring that the Roots Foundation Wales meets its legal obligations.
- The data protection officer is responsible for:

- Keeping the board of trustees updated about data protection responsibilities, risks, and issues.
- Reviewing all data protection procedures and related policies, in line with an agreed schedule
- 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 the Roots Foundation Wales holds about them (also called ‘subject access requests’)
- Checking and approving any contracts or agreements with third parties that may manage the organisation’s sensitive data.
- Approving any data protection statements attached to communications such as emails and letters.
- Addressing any data protection queries from journalists or media outlets like newspapers
- Where necessary, collaborating with other staff to ensure marketing initiatives abide by data protection principles.

- The appointed IT consultant 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 organisation is considering using to store or process data. For instance, cloud computing services

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. When access to confidential information is required, employees can request it from their line manager.
- The Roots Foundation Wales 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.
- 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 organisation 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.
- Employees should request help from their line manager or the data protection officer if they are unsure about any aspect 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 IT Consultant or data controller.

When data is stored on paper, it should 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?
- Employees should make sure paper, and printouts are not left where unauthorised people could see them, such as 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 should be protected by strong passwords that are changed regularly.
- If data is stored on removable media (like a USB or DVD), these should 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 an approved cloud computing services.
- Servers containing personal data should be sited in a secure location, away from general office space.
- Data should be backed up frequently. Those backups should be assessed regularly, in line with the organisation’s standard backup procedures.
- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.

- All servers and computers containing data should be protected by approved security software and a security system.

Data Use

Personal data is of no value to the Roots Foundation Wales 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 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 email, as this form of communication is not secure.
- Data must be encrypted before being transferred electronically. The IT Consultant can explain how to send data to authorised external contracts.
- Personal data should never be transferred outside of the European Economic Area
- Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

Data Accuracy

The law requires the Roots Foundation Wales 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 the Roots Foundation Wales 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 not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated. For instance, by confirming customers' details when they call.
- The Roots Foundation Wales will make it easy for data subjects to update the information the Roots Foundation Wales holds about them. For instance, via the organisation website.
- Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

Data Subject Access Requests

All individuals who are the subject of personal data held by the Roots Foundation Wales are entitled to:

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

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

Subject access requests from individuals should be made by email, addressed to the data controller at **office@roots.wales** The data controller can supply a standard request form, although individuals do not have to use this. The data should be specific and timelines to enable Roots to provide the specific data requested.

Individuals will be charged £10 per subject access request. The data controller will aim to provide the relevant data within one calendar month.

The data controller 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 Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.
Under these circumstances, the Roots Foundation Wales will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the organisation’s legal advisers where necessary.

Providing Information

The Roots Foundation Wales aims to ensure that individuals are aware that their data is being processed, and that they understand:

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

To these ends, the organisation has a privacy statement, setting out how data relating to individuals is used by the organisation.