

Fuse Rail needs to gather and use certain information about individuals. These can include customers, suppliers, business contacts, employees and other people that 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 that Fuse Rail:

- Complies with General Data Protection Regulations and follow good practice.
- Protects the rights of Employees, Sub Contractors, Customers, and partners.
- Is open about how it stores and processes individuals' data.
- Protects individuals rights in regard to how data is used and stored.
- Protects itself from Data Breach.

Data Protection Law

The overarching General Data Protection Act describes how organisations, including Fuse Rail, must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the regulations, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The General Data Protection Regulations are underpinned by the following important principles. They say that personal data must:

- Be processed fairly and lawfully.
Employees have the right to be informed about the processing of personal data.
- Be obtained only for specific, lawful purposes.
Employees have the right to restrict processing of their personal data if they consider that processing is unlawful or the data is inaccurate.
- Be adequate, relevant and not excessive.
- Be Accurate and kept up to date.
Employees have the right to rectification if personal data is found to be inaccurate or incomplete.
- Not be held longer than necessary.
Employees have the right to be forgotten by having data removed on request when there is no compelling reason for Fuse Rail to continue to process it.
- Processed in accordance with the rights of data subjects.
Employees have the right of access to their personal data and the right to confirm that their data is being processed.
- Be protected in appropriate ways.
Employees have the right to object to the processing of their personal data for direct marketing, scientific or historical research, or statistical purposes.
- Not to be transferred outside of the European Economic Area (EEA) unless that Country or Territory also ensures an adequate level of protection.
Employees have the right to data portability of their personal data for their own purposes.

Policy Scope

This Policy applies to:

- The Head Office of Fuse Rail.
- All Branches of Fuse Rail.
- All staff and volunteers of Fuse Rail.
- All contractors, sub-contractors, suppliers and any other people working on behalf of Fuse Rail.

It applies to all data that the company holds relating to identifiable individuals, even if that information falls outside of the General Data Protection Regulations. This can include:

- Names of Individuals
- Postal Addresses
- Email Addresses
- Telephone Numbers
- Any other information relating to individuals.

Data Protection Risks

This policy helps to protect Fuse Rail from some very real data security risks including;

- **Breaches of confidentiality**, i.e. information being given out inappropriately.
- **Failing to offer choice**, for instance unless data is being held for a lawful purpose, individuals should be free to choose how the company uses data relating to them.
- **Reputational damage**, i.e. Fuse Rail could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with Fuse Rail 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 Board of Directors are ultimately responsible for ensuring that Fuse Rail meets its legal obligations.

The Data Controller (HR Manager) is responsible for;

- Keeping the board 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 people covered by this policy.
- Handling data protection questions from staff and anyone else covered by its policy.
- Dealing with requests from individuals to see the data Fuse Rail holds about them (also called "subject access requests") within the timescales allowed by the General Data Protection Regulations.
- Checking and passing for final Directors approval any contracts of agreement with third parties that may handle company sensitive data.

The Managing Director 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 company is considering using to store or process data. For instance, cloud computing services.

The Finance and or Human Resources Manager is responsible for:

- Approving any data protection statements attached to communications such as emails & letters.
- Where necessary working with other staff to ensure marketing initiatives abide by data protection principles.

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 this should be requested through their line managers.
- Fuse Rail will provide information and, where necessary, training to all employees to help them understand their responsibility when handling data.
- Employees should keep all data secure, by taking sensible precautions. In particular strong passwords should be used and NEVER 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 any paper copies disposed of.
- Employees should request help from their line manager or the Data Controller (HR Manager) if they are unsure of 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 Manager 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 of 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, 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 should be protected by strong passwords that are changed regularly and never shared between employees.
- No data should be stored on removable media (like CD or DVD) or external hard drives.
- Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing services.
- Data should be backed up frequently. Those backups should be tested regularly.
- 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 an approved security software and a firewall.

Data Use

Personal data is of no value to Fuse Rail unless the business can make use of it. However, when personal data is accessed and used it can be at the greatest risk of loss, corruption and theft:

- When working with personal data employees should ensure the screens of their computers cannot be viewed by unauthorised personnel and that their screens are 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 should be encrypted before being sent electronically and only sent to authorise external contacts.
- Personal data should never be stored outside of the European Economic Area (EEA) unless that Country or Territory also ensures an adequate level of protection.
- Employees should never save copies of personal data to their own computers. Always access and update the central copy of any data.

Data Accuracy

The General Data Protection Regulations requires Fuse Rail 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 Fuse Rail 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 up to date and as accurate as possible.

- Data will only be held in as few places as necessary. Staff should not create any unnecessary additional files without consulting with Line Managers.
- Staff should take every opportunity to ensure data is updated. For Instance by confirming a suppliers or customers details when they call.
- Fuse Rail will make it easy for clients and suppliers to update the information that Fuse Rail holds about them for instance via the company's website.

Subject Access Requests

All individuals who are subject of personal data held by Fuse Rail are entitled to:

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

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

Subject Access requests from individuals should be made by email addressed to the Data Controller (HR Manager).

There is no charge for suppling this information except in limited cases where the request is found to be "manifestly unfounded or excessive" for example requests or grounds for refusal such as vexatious requests or repeated requests for the same information.

Under GDPR, responses to requests must be made without due delay and within one month of the original request for information being received.

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 Personal data may be disclosed to Law Enforcement Agencies without the consent of the data subject.

Under these circumstances Fuse Rail will disclose requested data. However the Data Controller will ensure the request is legitimate, seeking assistance from the board and legal advisers where necessary.

Providing Information.


Fuse Rail aims to ensure that individuals are aware that their data is being processed and they understand:

- How the data is being used.
- How to exercise their rights under GDPR.

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

REVIEW OF POLICY

This policy will be reviewed for adequacy and compliance to relevant standards.

Signed: 

Date: 27/01/25

D. Saunders, Managing Director