Data Protection Policy

Railmed+

Policy information	
Organisation	The Data Controller is the Occupational Health Manager.
Scope of policy	All medical and personnel records held in hard copy and electronic formats, as maintained by the Data Controller.
Policy operational date	6th January 2025
Policy prepared by	Compliance Manager
Date approved by the Managing Director	6th January 2025 No changes made

Review History	Signature
5/1/2026	

Data Protection Policy

Introduction	
Purpose of policy	• Complying with the law • Following good practice • Protecting clients, staff and other individuals • Protecting the organisation
Personal data	This includes hard copy medical records, including but not limited to: • Occupational Health Questionnaire & Assessments and attached printouts, • Drugs and alcohol reports, • Application forms that include staff addresses, bank details, and National Insurance Numbers etc.
Policy statement	Railmed is committed to: • Comply with both the law and good practice • Respect individuals' rights • Be open and honest with individuals whose data is held • Provide training and support for staff who handle personal data, so that they can act confidently and consistently • Registered with the Information Commissioner under the Data Protection Act 2018 / General Data Protection Regulation (GDPR) (EU) 2016.
Key risks	Main risks to Railmed: • Information about individuals getting into the wrong hands, through poor security or inappropriate disclosure of information • Individuals being harmed through data being inaccurate or insufficient

Responsibilities	
Trustees	The Managing Director has overall responsibility for ensuring that the business complies with its legal obligations.
Data Protection Officer **Data Controller**	The Occupational Health Manager is identified as the Data Protection Officer. Her responsibilities include: • Briefing the management and clerical team on Data Protection responsibilities • Reviewing Data Protection and related policies • Advising other staff on tricky Data Protection issues • Ensuring that Data Protection induction and training takes place, • Handling subject access requests • Approving unusual or controversial disclosures of personal data
Line Managers	Staff that handle personal data shall comply with this Policy and all supporting management system procedures to ensure that good Data Protection practice is maintained. This includes induction and training records etc. Also, staff must ensure that the Data Protection Officer is informed of any changes in their uses of personal data that might affect the Company's Notification.
Enforcement	The penalties levied on the Railmed and individuals within the Company for infringing the Data Protection may include an unlimited fine and compensation paid to the damaged party. Under GDPR organizations in breach of GDPR can be fined up to 4% of annual global turnover or €20 Million (whichever is greater). This is the maximum fine that can be imposed for the most serious infringements e.g. not having sufficient customer consent to process data or violating the core of Privacy by Design concepts.

Confidentiality	
Scope	As part of this Policy, confidentiality shall be limited to personal data covered by the Data Protection Act 2018, the General Data Protection Regulation (GDPR) (EU) 2016 and Medical Records Act 1998. GPDR will apply to the processing of personal data of data subjects in the EU by a controller or processor not established in the EU, where the activities relate to: offering goods or services to EU citizens (irrespective of whether payment is required) and the monitoring of behaviour that takes place within the EU.
Understanding of confidentiality	Railmed shall ensure that personal data is not disclosed or access made available to such data to persons that have no authority to see such data. There will always be cases where the Railmed feels it is right to break confidentiality, although this should be decided on a case-by-case basis whether this is appropriate. Access to medical records shall be limited to medical assessment personnel (including specialist suppliers) and the Administrator. Access to personnel and financial records shall be limited to the Managing Director, the Administrator and the Occupational Health Team, i.e. on a "need to know" basis; no one should have access to information unless it is relevant to their work.
Communication with Data Subjects	Staff shall be informed about confidentiality of their personnel and financial record, so that there is minimal risk of them being surprised at any later stage to find out that who has information about them. Outside parties that attend a Railmed medical assessment and/or drugs & alcohol screening shall be informed about confidentiality at the time of the assessment / screening, so that there is minimal risk of them being surprised at a later stage to find out that their Employer, Network Rail, London Underground and Sentinel has information about them.
Communication with staff	All staff that process and maintain personal data on individuals shall receive appropriate training and information to enable them to undertake their duties in-accordance with Company policies and procedures, and specifically whether information should be disclosed, or access allowed.

Security	
Scope	Security shall be applied to all personnel, training and medical fitness records.
Setting security levels	Security levels include: • The communication of personal data over the phone, • The transmission of personal data via fax or email, • Desktop security, where hard copy and electronic personal data may be left on the desk or displayed on the screen by authorised staff, and where unauthorised staff or outside parties may view or remove such data, • The transport of paper records by vehicle, • The storage of electronic data / records, • The transfer of records upon request to a new Occupational Health provider.
Security measures	Security measures shall include but not limited to: • Training and instruction to staff to prevent personal data being disclosed over the phone, without establishing the caller's authorisation to have the data, • Call back process, to ensure he requesters identity is verified before disclosing data, • Faxed personal; data is only sent once the recipient has confirmed they are by the receiving fax, • Fax headers to clearly state the data being sent is confidential, • Screen savers and password protection set up to ensure inactive screens do not display data, • Promote and monitor a clear desk policy, to ensure personal data is not left unattended, • Paper records to be stored out of sites when transporting these by vehicle, and the vehicle doors to be locked and the immobilizer / alarm activated when leaving the vehicle for any length of time, • Ideally paper records should not be stored overnight in a vehicle, • Server networks and databases shall be protected by appropriate security software / firewalls, • The uploading of software onto server networks must be authorised by the Managing Director or Compliance Manager, • All requests for the transfer of records a new Occupational Health provider must be made in writing and confirmed with the sponsor prior to the transfer taking place.

Business continuity	The Company shall maintain all personnel, training and medical fitness records in secure filing cabinets, and the offices shall be alarmed against intruders and fires. Where applicable, electronic registers, database, training and medical fitness logs shall be retained on the Company computers, which is backed-up regularly, with the back-ups held off-site.
Specific risks	Staff may be tricked into giving away personal data by phone or e-mail. Staff shall receive guidance for dealing with these threats.

Data recording and storage	
Accuracy	Where information is taken over the telephone, it shall be checked back with the person by repeating the information, and where appropriate confirmed in writing. If information is supplied by a third party, the accuracy of the information shall be checked for errors or omissions and to ensure it is legible.
Storage	All hard copy personal data shall be stored in secure cabinets / cupboards at Lawrence House. Data held electronically, shall be restricted to authorised personnel only, and protected by password.
Retention periods	Personnel and training data shall be held for the duration of an individual's employment then retained as an archive record for at least five years. Medical and screening records shall be retained as an archive record for at least ten years from the date of the appointment, and positive results shall be retained indefinitely.
Archiving	Hard copy archive records shall be held in dated storage boxes that details the records enclosed. The boxes shall be held securely and protected from damage or deterioration. Electronic held records shall be held on appropriate memory devices such as memory sticks, with a register maintained for each device or disc. The devices shall be held securely and protected from damage or deterioration. The content of the archive storage boxes shall be checked at least annually. Records passed their retention period shall be destroyed through shredding or incineration.

Subject access	
Responsibility	All requests for access to personal data must be processed by the Occupational Health Manager who is responsible for ensuring that subject access requests are handled within the legal time limit of 40 days.
Procedure for making request	Subject access must be in writing to the Occupational Health Manager. The Manager shall review the request and confirm receipt in writing to the requester. As requests are infrequent and can be complex, the Manager may seek legal advice before agreeing to release the data.
Provision for verifying identity	Before handing over any personal data, the Requester shall be required to provide roof of identity using photographic identification. This may include a UK Passport, or UK Driving Licence etc.
Charging	The Railmed reserves the right to charge a £10 administration fee, which shall be clearly detailed in the confirmation letter, which shall have an invoice attached for payment.
Procedure for granting access	The provision of the data shall normally be as a hard copy (in permanent form) format. Supervised access in person may be arranged for certain types of data.
Removal of Harmful Information	Prior to the release of personal data to the requester, the Company shall ensure this data has been reviewed by an authorised person so that harmful information and references to other people are removed. In the case of medical records, the data shall be reviewed by the Responsible Authorising Physician. In the case of personnel and financial records, the data shall be reviewed by the Occupational Health Manager.

Transparency	
Commitment	Railmed is committed to ensuring that in principle staff and other individuals are aware that their data is being processed and • For what purpose it is being processed • What types of disclosure are likely, and • How to exercise their rights in relation to the data
Procedure	This shall be achieved through the Company Induction process for staff. Other individuals shall be informed in a manner appropriate to the type of data being held, e.g.: • Booking confirmation • Information sheets • Consent forms
Responsibility	The Managing Director is responsible for ensure all staff are inducted into the Company. The Administrator and Occupational Health Team team are responsible for ensuring Candidates / Donors are suitably informed and sign the appropriate consents and acknowledgements.

Consent	
Underlying principles	Consent from the individual is one way of complying with the Fair Processing Conditions covered under the Data Protection Act 2018 / General Data Protection Regulation (GDPR) (EU) 2016. Personnel records shall only be disclosed to other Railmed staff in order to arrange a method for payment and for communicating important safety information. In such cases, no consent is formally requested. Where outside parties request personal information, this shall not be disclosed without written consent from the staff. All persons attending a medical assessment and/or drugs & alcohol screening shall be required to sign consent before the procedures are carried out.
Withdrawing consent	Railmed acknowledges that, once given, consent can be withdrawn, but not retrospectively. There may be occasions where Railmed has no choice but to retain data for a certain length of time, even though consent for using it has been withdrawn.

Staff training & acceptance of responsibilities	
Documentation	Staff responsibilities regarding Data Protection are detailed within their agreed Job Descriptions.
Induction	All staff who have access to any kind of personal data are briefed against their Job Descriptions as part of their Company Induction.
Continuing training	Data Protection issues shall be communicated through training, team meetings, and supervisions etc.

Policy review	
Responsibility	The Managing Director is responsible for reviewing the Policy at least annually.
Procedure	The review shall take place at the Annual Management Review Meetings, which must be chaired by the Managing Director, attended by at least one of the management team.
Timing	Annually.

Signed.....
Managing Director

6th January 2025
No changes made

Notes

Data Controller

The Data Controller is the legal 'person' responsible for complying with the Data Protection Act 2018 / General Data Protection Regulation (GDPR) (EU) 2016.

Fair processing conditions

Schedule 9 of the Data Protection Act lays down six conditions, at least one of which must be met, in order for any use of personal data to be fair. These are (in brief):

1. The data subject has given consent to the processing,
2. The processing is necessary—
   (a) for the performance of a contract to which the data subject is a party,
   or
   (b) in order to take steps at the request of the data subject prior to entering into a contract.
3. The processing is necessary for compliance with a legal obligation to which the Controller is subject, other than an obligation imposed by contract.
4. The processing is necessary in order to protect the vital interests of the data subject or of another individual.
5. The processing is necessary—
   (a) for the administration of justice,
   (b) for the exercise of any functions of either House of Parliament,
   (c) for the exercise of any functions conferred on a person by an enactment or rule of law,
   (d) for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or
   (e) for the exercise of any other functions of a public nature exercised in the public interest by a person.
6. (1) The processing is necessary for the purposes of legitimate interests pursued by—
   (a) the controller, or
   (b) the third party or parties to whom the data is disclosed.

Subject access

Individuals have a right to know what information is being held about them. The basic provision is that, in response to a valid request (including the fee, if required), the Data Controller must provide a permanent, intelligible copy of all the personal data about that Data Subject held at the time the application was made. The Data Controller may negotiate with the Data Subject to provide a more limited range of data (or may choose to provide more), and certain data may be withheld, especially if this is likely to cause harm or distress to a person. This also includes some third-party material, especially if any duty of confidentiality is owed to the third party, and limited amounts of other material. ("Third Party" means either that the data is about someone else, or someone else is the source.)

Health & Safety Policy Statement

Railmed+

Railmed Ltd Policy is to promote a Health and Safety culture throughout the organisation, which aims as far as reasonably practicable towards the prevention of injuries and ill health of employees and others who may be affected by our work activities and to prevent any loss or damage to property and equipment. This shall be achieved and maintained by involving all levels of employees in systematically identifying workplace hazards, making adequate assessments and taking appropriate steps to set up safe systems of work, which control risks associated with the provision of occupational health services.

People are our key resource and Railmed is committed to adequately re-sourcing all areas of its operation.

We believe that excellent Health and Safety standards shall contribute towards the development of our staff and lead to excellent business performance. Accordingly, we shall support Health and Behavioural Safety initiatives, aimed at continuous improvement of our management system and the safety culture within our business, in which Health and Safety objectives are regarded by all as an integral part of our overall business goals.

Health & Safety will never be compromised for other objectives.

The Company recognizes its legal responsibilities under the Health and Safety at Work Act 1974 and its associated underpinning regulations. Accordingly, the Managing Director has overall responsibility for policy formulation, development and implementation. The Company considers that Health and Safety legislation provides only the minimum standards and shall continually seek to improve upon those legal requirements.

We shall ensure that all employees are informed about the Policy and its mandatory compliance. We shall consult with them on its implementation and their own individual Health and Safety responsibilities. All employees shall be provided with the appropriate training so that they can fulfil their Health and Safety responsibilities. The principle operational responsibility for Health and Safety and for the implementation of this Policy lies with all employees. An appropriate number of Health and Safety advisers and representatives with a specific role shall be appointed to provide independent and authoritative advice to management.

We shall continuously monitor Health and Safety performance to ensure that standards are met and management controls are working. The Company's policy and safety performance shall be reviewed, as a minimum, annually. Revisions to the Policy shall be implemented as a result of any deficiencies highlighted by the review, or by new legislation and rail Standards, or by business development.

The Company is committed to the success of this Policy.

Signed.....

Managing Director

6th January 2025

No changes made

Review History	Signature
5/1/26	

Alcohol & Drug Policy Statement

Railmed+

Railmed Ltd has a zero-tolerance policy with regards to Alcohol and Drugs.

Possession, intoxication or use of alcohol or non-prescribed drugs on Company premises, or whilst on Company business will be considered gross misconduct and will be subject to disciplinary action.

Persons suspected of being under the influence of alcohol or non-prescribed drugs will be subject to an alcohol and drug test. Failure to give a sample will lead to disciplinary action being taken.

Persons undergoing investigation for alcohol or drugs will be suspended from work with immediate effect pending the required testing. On completion of any test taken, if the employee tests positive for alcohol non-prescribed drugs, the employee's contract will be terminated with immediate effect.

It is a requirement of the Company that no employee shall:

- Report or endeavour to report for duty having just consumed alcohol or under the influence of drugs.
- Report for duty in an unfit state due to the use of alcohol or drugs
- Be in possession of non-prescription drugs in the work place
- Consume alcohol or drugs whilst on duty

In addition, staff are required to report when they are taking prescribed or 'over the counter' medication, which may affect their activities.

The Company will not tolerate any deviation from these rules and will take appropriate action in the event of any infringement. The Company has a policy of assistance with the rehabilitation of staff who voluntarily seeks help for alcohol or drug related problems. Such staff must, however, seek assistance at the earliest opportunity; subsequent discovery or a disclosure prompted by impending screening will not be acceptable.

Every measure will be taken to ensure that all employees are made aware of this statement and its content and that it is adhered to.

Signed.....

Managing Director

6th January 2025

No changes made

Review History	Signature
5/1/26	

Environmental Policy Statement

Railmed+

Railmed Ltd is committed to the identification of environmental aspects of its activities and services and minimising the environmental impact to its railway Clients throughout their lifecycle.

Railmed aim to:

- Continually improve its environmental performance through the development and achievement of objectives and targets.
- Prevent pollution of the environment and have procedures in place to deal with environmental accidents.
- Comply with all relevant environmental legislation.
- Improve and integrate, where possible, environmental management into our business systems.
- Ensure that effective relationships are maintained with industry partners, regulatory bodies and other interested parties.
- Examine our use of resources, plant, and materials, and seek to minimise use and recycle or reuse waste where practicable.
- Involve all staff in the promotion of Railmed attitude to the environment, through environmental awareness, training and guidance.

The transportation and disposal of all wastes will be carried out in a responsible manner with due regard to environmental consideration and all current legislation.

Our investment policy and control measures consider all national interpretations of the "Best Practicable Environmental Options".

The Company recognizes its legal responsibilities under the Environmental Protection Act 1990 and its associated underpinning regulations. The Managing Director is responsible for the implementation of the Company's environmental policy. This policy shall be briefed to all Railmed employees and made available to the public. The requirements of this policy shall be reviewed on a regular basis, but at least annually.

Signed.....

Managing Director

6th January 2025

No changes made

Review History	Signature
5/1/26	

Quality Policy Statement

Railmed+

The Company is dedicated to the quality policy that will ensure that its services fully meet the requirements of its Customers at all times. The goal of the Company is to achieve a high level of customer satisfaction at all times. Commitment to the implementation of supporting managerial and business operational systems is essential to realising that goal.

Railmed Ltd believes in the concept of Client and supplier working together in pursuing this policy and continual improvement in quality performance.

The quality policy is based on the following principles:

1. Ensuring that we fully identify and conform to the needs of our Customers,
2. Looking at our service provision processes, identifying the potential for errors and taking the necessary action to eliminate them,
3. Everyone understanding how to do their job and doing it right first time,
4. Working with suppliers and Customers to establish and maintain the highest quality standards.

To ensure that the policy is successfully implemented, staff will be responsible for identifying Customer requirements, and ensuring that the correct procedures are followed to meet those requirements.

Objectives needed to ensure that the requirements of this policy are met and that continual improvement is maintained in line with the spirit of the policy, will be set, determined and monitored at Management Review.

The quality policy principles and objectives will be communicated and available to staff at all times. Training will be an integral part of the strategy to achieve the objectives.

Within this Policy we are committed to operating our Company under the disciplines and control of a management system conforming to the International Standard BS EN ISO9001. While the Company is committed to operating continuously to this standard, it has no immediate plans to certificate the management system through an independent organisation.

Our Company will constantly review and improve on our services to ensure tasks are completed in the most cost effective and timely manner for the benefit of all our Customers.

We shall ensure that all our personnel understand and fully implement our Company's policies and objectives and are able to perform their duties effectively through an ongoing training and development programme.

Signed.....

Managing Director

6th January 2025

No changes made

Review History	Signature
5/1/26	

Security Policy Statement

Railmed+

The safety and security of our employees and assets is a top priority. We shall ensure that comprehensive security measures are put in place to protect our employees, assets, and the industry in which we work.

We shall implement processes to identify security threats and risks, implement effective prevention measures and safeguard our employees, assets and information. This allows us to create a safe and secure environment that protects our business and its stakeholders, as well as our brand and reputation.

The key elements of the Policy are:

Identification of risks

We shall identify security risks to employees, assets, operations, information and reputation, in order to put in place effective prevention measures. In doing so we will consider all risks that emanate from economic, technological and social factors, and take appropriate measures to minimise these risks.

We shall also assess whether actions of the company or employees heighten risk and act appropriately to minimise any such risks whilst raising awareness amongst our employees.

Investigation and action against security incidents

We will investigate security incidents appropriately and take necessary action to minimise the probability of recurrence.

We will also investigate and manage expeditiously security related grievances that may be raised by employees or customers and other parties.

Local law enforcement partnerships

We will work with local law enforcement authorities to ensure appropriate responses to security incidents involving Railmed personnel or assets.

Personal accountability

We will promote personal accountability by taking corrective and/or disciplinary action against Railmed employees breaking the law or violating their terms of employment.

Respecting the communities in which we operate

While implementing the security policy we will aim to minimise the risk to our Customers and the local communities around our depots and worksite, and engage in dialogue with them to ensure adequate prevention measures are in place.

6. Communications

We will communicate this policy to employees as part of the Company induction process.
We will also communicate this policy to our suppliers, customers and wider stakeholders.

Signed.....

Managing Director

6th January 2025

No changes made

Review History	Signature
5/1/26	