**CANDIDATE PRIVACY POLICY**

Merseyrail provides this Candidate Privacy Notice to make aware of how and why your personal data will be used in our recruitment of staff.

Merseyrail are committed to protecting and respecting your privacy. This Candidate privacy notice explains how we collect and use personal information about you during the recruitment process in accordance with the UK General Data Regulation (UK GDPR).

**CONTENTS**

* what personal data we collect from you when you apply for a position with us;
* how we collect and use that information;
* the purposes and legal basis for our use of the information;
* where we store your information securely; and
* your rights in relation to the information we hold.

**The law in the UK requires us to let you know that the data controller is:**

Merseyrail Electrics 2002 Ltd

9th Floor, Rail House, Lord Nelson Street, Liverpool, L11JF

**Our Data Protection Manager (DPM) is:**

Joseph Williams

8th Floor, Rail House, Lord Nelson Street, Liverpool, L11JF

Privacy@merseyrail.org

**Our Data Protection Officer (DPO) is:**

Transport UK Group

2nd Floor, 18-20 St Andrews Street, London, EC4A 3AG

dpoabellio@abellio.com

**PERSONAL DATA WE MAY COLLECT FROM YOU**

We may process the following types of information about you:

* "Contact Information" means your name, your address, your telephone number and your personal email address;
* "Recruitment Information" means your application form, CV, details of your professional qualifications and any references received, right to work documentation
* "Identity Information" means information about you, such as your age, date of birth, country of residence, medical conditions, allergies, passport details, marital status, photographs details of dependents and next of kin;
* "Background Information" means criminal background checks or other background checks carried out by us;
* "Payment Details" means payment records, national insurance number, bank account details, tax details
* "HR Records" means holiday, sickness or other absence records, performance records, records relating to benefits such as pension and health insurance;
* "Preferences Data" means data about your preferences in relation to information we contact you with; and
* "CCTV Data" means images of you that are captured on CCTV systems that are in operation inside of our office building, at our stations or on our trains. (Whether operated by the Company, on our behalf or to which we have access).

The personal data that we collect about you may also include special categories of personal data, such as information about your racial or ethnic origin, criminal or alleged criminal offences, sexual orientation or your health and lifestyle, where applicable to the recruitment process including where necessary to accommodate any disability needs. If you fail to provide us with this information, or you object to us processing such information, the consequences are that we may be prevented from progressing your application.

**HOW WE COLLECT YOUR DATA**

* When you apply for a job with Merseyrail
* We may process data that you make public via social media (such as LinkedIn)
* We may obtain your data through third parties (such as recruitment agencies)

If successful in the employment process any information provided through the recruitment process may form the basis of your personnel record with us and may be used for the purposes of administering your employment, benefits and training with the firm, ensuring your health and safety and to fulfil our responsibilities as an employer. You will receive further information about such processing as applicable.

**LEGAL REASONS FOR USING YOUR DATA**

We may use your data in a variety of ways. In each instance, we rely on an appropriate lawful basis defined by the UK GDPR or other data protection law. For example ;

* Contractual obligation: which means our processing of your personal information is necessary for performance of contracts to which you will be a party to or in order to take steps at your request prior to you entering into those contracts
* Legal obligations: for payment of tax, verifying employee qualifications for the role, Health and Safety, Regulatory Compliance (Department for Transport (DfT), Office of Rail and Road, etc);
* Legitimate interests: which means our processing is necessary for the purposes of legitimate interests pursued by us. Our legitimate interests are that we are conducting the processing: (i) to run and administer the business of the Company, (ii) to uphold or enforce our professional, legal and regulatory obligations, working practices, standards, policies and procedures (including any sickness policy or working time policy), (iii) managing the employment (or equivalent) of Staff and (iv) evaluating the Company’s recruitment practices and procedures.

**Special Categories of Personal Data**

You may also supply us with special categories of personal data (including your racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health and sexual orientation. This is gathered for the following purposes:

* equal opportunity monitoring purposes
* to assess suitability for roles
* to consider whether adjustments may need to be made to accommodate employees with a disability
* protect the safety and security of our candidates, staff, customers, and the general public.
* management of the employment in relation to health consideration, including providing benefits such as medical insurance.

If provided voluntarily for equal opportunity purpose, we may request consent and use the data to monitor our equality and diversity and make improvements.

We may also collect and use details of criminal records/proceedings, where applicable to your role, for example in carrying out a DVLA check for a driver

**PURPOSE FOR COLLECTING YOUR DATA**

We will only use the information you provide as permitted by Data Protection Law (DPL). Our reason(s) for using your data will vary.

* To consider and process any application that you make for any job with us
* To determine whether you have the profession skills, expertise and experience for the position applied for
* To verify your identity, address, right to work, employment history and criminal background
* To assist in the administration of our recruitment programme, recruitment campaign planning and compliance with related internal policies.
* To provide you with information about other job vacancies if you would like us to send you such notifications
* To consider job suitability under occupation health and safety

**DATA WE SHARE**

We may share or disclose information for the following reasons:

* We will share the information with organisations that we outsource parts of our HR work. This includes cloud-based storage and processing facilities, recruitment payroll, pension services and other Group Companies. Some cloud providers host their services outside of the EEA, including the USA. Where personal data is exported out of the EEA, we use either model contract clauses or similar, to achieve adequacy requirements
* Where you wish to access benefits, we provide such as private health care and occupational health providers
* To comply with legal or other obligations for example, relating to crime and taxation purposes or regulatory activity, such as operating PAYE.
* For our legitimate business interests, such as, running and improving the business, occupational health and safety requirements, security, fraud prevention, revenue protection or developing new services.
* Where required with DfT or a successor franchisee because of the sale, merger, or acquisition of business assets
* To carry out equalities monitoring

**Information for Data Subjects in the EEA or UK**

When we, or our permitted third parties, transfer your information outside the UK or EEA, we or they will impose contractual obligations on the recipients of that data to protect your information to the standard required in the UK or EEA. We or they may also require the recipient to subscribe to international frameworks intended to enable secure data sharing. In the case of transfers by us, we will only transfer your information outside of the UK or EEA where:

* the transfer is to a country deemed by the UK Government or European Commission to provide adequate protection of your information;
* where you have consented to the transfer; or
* where such transfer is otherwise permissible under Data Protection Legislation (for example where we are required to provide such information by law or where relevant contractual arrangements have been entered into between the parties (as described above)).

**CCTV**

***Camera systems we operate***

Our CCTV is used to capture, record and monitor images of what takes place on our premises and property, in real time.

Depending on the type of camera, images are recorded on video tape (analogue) or as digital data. Cameras can be fixed or set to scan an area. In some circumstances, they can be operated remotely by controllers.

***Why we operate CCTV cameras***

We operate CCTV for the following purposes:

* Health and safety of employees, passengers and other members of the public; and
* Prevention and detection of crime and anti-social behaviour.

***Camera locations***

We operate cameras at our stations and on all the trains that we run.

***Length of time CCTV footage is kept***

CCTV footage at stations is generally held for a maximum of 31 days from the time of recording.

Recordings from body worn cameras is generally held for 31 days, unless required for legitimate business reasons.

CCTV footage from our trains is kept for a maximum of 7 days.

Where CCTV footage is required to assist with the investigation of an accident, allegations of criminal activity or our other legitimate business purposes it will be downloaded and securely stored in line with our retention policy.

***How to access your CCTV personal data***

You can request copies of images or footage of yourself by making a request using the contact details set out below.

***Disclosing CCTV/personal data to the police***

At our discretion, we may disclose CCTV in response to valid requests from the police and other statutory law enforcement agencies.

Before we authorise any disclosure, the police have to demonstrate that the CCTV recording is necessary to assist them in the prevention or detection of a specific crime, or in the apprehension or prosecution of an offender.

Requests from the police are dealt with on a case-by-case basis to ensure that any such disclosure is lawful in accordance with the Data protection Laws.

***Sharing CCTV footage with other third parties***

We may share CCTV images with the Department for Transport to support investigations into major incidents involving us.

We may also disclose personal data to third parties, if required to by law or it is necessary for a legitimate purpose such as defending or bringing legal action. UK law allows us to do this where the request is supported by:

* evidence of the relevant legislation;
* a court order; or
* satisfactory evidence and assurances of the legitimate interest.

Legitimate interest would include requests such as defending or making a legal claim, such as to insurers following an incident. When we are not required to provide CCTV, we will take into account the circumstances and any potential harm to individuals, we may also charge a fee and seek indemnity for any use beyond which it is requested.

***External guidelines and best practice***

We operate our CCTV systems in compliance with the CCTV Code of Practice issued by the Information Commissioner’s Office (ICO). The Code describes best practice standards which should be followed by organisations operating devices which view or record images of individuals. It also covers other data derived from those images that relates to individuals (for example vehicle registration marks).

**INFORMATION SECURITY**

We use a range of appropriate technical and organisational measures to safeguard access to and use of, your personal information and to ensure it retains its integrity and availability. These include structured access controls to systems, network protection, intrusion detection, physical access controls and staff training. We also consider anonymising or pseudonymising personal data where practical.

Although we maintain physical, electronic, and administrative safeguards to protect your personal information from unauthorised or inappropriate access, the transmission of information via the internet is not completely secure and we cannot guarantee the security of your personal information transmitted to us or provided through email or portals. Personal information that you submit may be sent to, and stored on, secure servers owned by or operated for us by third-party providers. Any payment transactions carried out by our chosen third-party provider will be encrypted using appropriate technology. We may collect and store personal data on your device using application data caches or browser web storage, if you use those devices for a work purpose.

**YOUR RIGHTS**

To the personal data we hold about you

You have several rights concerning the way that we use your information.

**RIGHT TO OBJECT TO DIRECT MARKETING**

To prevent marketing to you, you have the right to ask us not to process your personal information for marketing purposes. We will usually inform you before collecting your information if we intend to use or disclose it for such purposes. If you do not want us to use your information for marketing purposes either:

* indicate this by NOT ticking the box to be sent marketing emails (or offers);
* click the unsubscribe link on direct marketing emails; or
* contact us

**RIGHT TO BE INFORMED AND RIGHT OF ACCESS**

You have the right to be told what information we hold about you. You are also able to request a copy of your personal information. We may need to ask for some further information, such as checking who you are. Please let us know in what format you wish to receive your information.

**RIGHT OF RECTIFICATION and RIGHT OF RESTRICTION**

If you believe the information, we hold about you is inaccurate or incomplete you can contact us and ask us to correct it. You may also request any data processing we are carrying out on your data is halted whilst a request for rectification, objection, or a dispute over the lawfulness of processing is being considered. We will provide a response confirming the action we have taken or disagree with taking.

**RIGHT OF ERASURE**

This is also known as the “Right to be forgotten”, you can request deletion or removal of personal information in some circumstances, such as where there is no compelling reason for its continued processing. We will also take reasonable steps to notify third parties of your instruction and request that they act upon it, in a similar manner.

**WITHDRAWAL OF CONSENT**

If we relied on consent as the ground for processing your personal data, you can withdraw this consent at any time. It does not affect the processing carried out beforehand. You can withdraw consent by contacting Customer Relations on 0151 555 1111 or our Data Protection Manager on Privacy@merseyrail.org

Where you have consented to receive direct marketing communications, you can withdraw your agreement at any time, as above or by clicking on the appropriate link in any Merseyrail email. We will act upon such an instruction as soon as possible.

**AUTOMATED DECISION MAKING**

The GDPR sets out several obligations and restrictions in respect of any automated decision making. However, Merseyrail does not conduct any automated decision-making activities.

**PORTABILITY**

Where you have provided us with personal data and the reasons, we are processing it are based on consent or our contract with you, and the processing is automated, you have a right to ask for that information be provided to you or another data controller in a structured, commonly used and machine-readable format. The right may be restricted if it is not practical for us to provide the information in this way or it adversely affects the rights of others.

**HOW WE DEAL WITH RIGHTS REQUESTS**

We are not able to charge you a fee for dealing with rights requests, unless they are manifestly unfounded or excessive or in circumstances where copies have been provided previously. We would always let you know if we thought this was the case, so that you can make a decision about what you wanted to do next.

There are various limitations and exemptions in relation to the exercise of rights in Data Protection Legislation – for example if it would affect another’s rights and freedoms or if we need to retain the information to make or defend a legal claim. We intend only to rely on limitations and exemptions where it is fair to do so and always bearing in mind that it is your personal data.

**Timeframes**

If you wish to exercise any of these rights, please contact Privacy@merseyrail.org. Unless stated otherwise we will aim to satisfy your instruction without undue delay and within 1 month. If we anticipate that we will not meet with this timeframe we will let you know within that period to explain what the problem is.

**HOW LONG DO WE KEEP YOUR PERSONAL DATA FOR?**

If your application for employment is unsuccessful then we may continue to hold information and opinions about you and your applications after any application process is complete, in case we need to consult it in the future if you make another application or become an employee, if a dispute arises about an application that you have made or in order to contact you if potentially suitable job opportunities become available in the future.

We will delete or anonymise your information after [6] years, or sooner if we no longer need it, although we may continue to hold purely statistical information which does not identify you.

**OPT OUT**

If you have registered to receive job vacancy updates by email, we will send you such updates. If you no longer wish to receive these, you can request that we amend your preferences by contacting us on the email below

**COMPLAINTS**

If you are not happy with the way in which we deal with your data or have dealt with a rights request, then please us know. Our Data Protection Manager role has been established in a manner to remain independent of business decisions, and is the first point of contact for dealing with Rights Requests and complaints.

**Our Data Protection Manager (DPM) is:**

Joseph Williams, 8th Floor, Rail House, Lord Nelson Street, Liverpool, L11JF, Privacy@merseyrail.org

If you are not satisfied with the way in which our DPM has handled your complaint or rights request, then you can contact our Group Data Protection Officer.

**Our Data Protection Officer (DPO) is:**

Transport UK Group, 2nd Floor, 18-20 St Andrews Street, London, EC4A 3AG

dpoabellio@abellio.com

If you are not satisfied with our DPO’s response you can complain to the ICO. Their contact details are:

Head Office, Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Tel: 0303 123 1113 (local rate) or 01625 545 745 if you prefer to use a national rate number

Fax: 01625 524 510

<https://ico.org.uk/global/contact-us/>

**CHANGES TO THIS PRIVACY POLICY**

We may revise this Privacy Policy from time to time. The most current version of this policy will govern use of your information and will always be available on request.

This Policy was last updated in Jan 2023.