

CUSTOMER PRIVACY NOTICE

Merseyrail “we” “us” provides this Customer Privacy Notice to make you aware of how Merseyrail is committed to respecting your data privacy whilst using our services.

CUSTOMER PRIVACY NOTICE

Your personal data is important. So important that there are a range of laws in place to safeguard your data (the most important being the General Data Protections Regulation "GDPR". Merseyrail are committed to doing its part in protecting and respecting your privacy when you use our services, and we value the personal Data you provide to us and comply with those laws.

In practice, this means that all personal data which we hold about you will be

- Used lawfully, fairly and in a transparent way
- Collected only for valid purposes that we have clearly explained to you and not used in a way which is incompatible with those purposes
- Relevant to the purposes we have told you about and limited only to those purposes.
- Accurate and kept up to date
- Kept only as long as necessary for the purposes we have told you about
- Kept securely

This Privacy Notice explains:

- what personal data we collect from you when you use our website, apps, contact us, travel on our trains, use our services or WiFi;
- how we collect and use that Data;
- the purposes and legal basis for our use of the Data;
- how we keep Data secure; and
- how you can contact us if you wish to exercise any of your rights in relation to the Data or make a complaint.

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

Merseyrail Electrics 2002 Ltd
Railhouse, Lord Nelson Street, Liverpool
L11JF

Our Data Protection Officer is:

Abellio

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

Dpoabellio@abellio.com

More information about data protection law in the UK and what that means for you can be found on the Information Commissioner's Office website: <https://ico.org.uk/>

HOW WE COLLECT YOUR DATA

We may collect and process data about you when we have direct interactions with you. This might include where you:

- buy tickets;
- travel on our services;
- use our Website, Apps or WIFI;
- contact Customer Relations;
- enter a competition, promotion or survey; or
- lose property on our premises;
- where you are on our property through CCTV or body worn video.
- are involved in an accident or incident on our network
- are in breach of Merseyrail byelaws or any other applicable law

We may also process personal data that you choose to make public including via social media.

We may also collect personal data through automated technologies or interactions with our Website, Apps and WiFi.

Sometimes we obtain your personal data through third parties who provide your data to us. This might include other members of our Group as well as our service providers.

THE DATA WE COLLECTED ABOUT YOU

“Personal Data” means any Data about an individual from which that person can be identified. It does not include data where the identity of the person concerned has been removed (Which is called “Anonymised Data”)

We may collect, use, store, transfer different kinds of personal data about you. This can be broken down to the following categories Data "**Contact Data**" means your first and last name, your address, your telephone number and your email address;

- **"Profile Data"** means your username, password and other registration Data used on our Apps, Website or WiFi;
- **"Identity Data"** means Data about you, such as your age, date of birth, country of residence, medical conditions, allergies, passport details, details of trains you have travelled on or financial Data;
- **"Communication Data"** means Data in connection with communications you send us, for example, to report a problem or submit queries and might include voice recordings of telephone calls;
- **"Data and Usage Data"** means data about how you use our Apps, Websites or WiFi, including details of the functions and services you use, your visits to our media, traffic data, and location data;
- **"Technical Data"** means Data about the type of internet browser and operating system you use, your device's IMEI number, the MAC address of the device's wireless network interface, mobile network Data and the time zone setting;
- **"Marketing and Communications Data"** includes your preferences in receiving marketing from us and our third parties and your communication preferences; and
- **"Cookie and Tracker Data"** means Data we collect through cookies and similar technologies, which may include Data and Usage Data and Technical Data.

LEGAL REASONS FOR USING YOUR DATA

We will only use the Data you provide as permitted by law. With that in mind, we shall only process your personal Data where we have a legal basis for doing so. These legal bases are:

- **Contractual obligation** which means our processing of your personal data is necessary for performance of contracts to which you will be a party to and in order to take steps at your request prior to you entering into those contracts
- **Legitimate interests** which means our processing is necessary for the purposes of legitimate interests pursued by us. Primarily our legitimate interests are to provide our services to you or our other customers.
- Other legitimate interests are that we are conducting the processing to make sure:
 - (i) we provide sustainable and high quality, locally focused passenger transport services;
 - (ii) we improve and expand our services;
 - (iii) we are a leading employer in the transport sector, investing in and developing our staff;
 - (iv) we operate with financial discipline and reducing crime and fraud to provide shareholder value;
 - (v) our Website, Apps or Wifi or our property is safe, efficient and customised;
 - (vi) you receive updated data on our business activities;
 - (vii) to provide the services you have requested;
 - (viii) to ensure that the content on our Website or Apps is presented in the most effective manner for you and your device;
 - (ix) to allow you to participate in any features on our Website or Apps when you choose to do so; and
 - (x) for our own marketing and research
- **Legal obligation** which means our processing is necessary for us to comply with the law or a court order.
- **Consent** which means you have provided your consent to our processing and, in the context of this Privacy Notice, shall only relate personal data we collect and process through cookies and similar tracking technologies. For more information on cookies, please refer to our Cookie Notice.

Our reasons for using your data as well as why we are permitted to do will vary but might include:

Purpose	Categories of personal data	Legal Basis
To provide services to our customers	<ul style="list-style-type: none">• Contact Data• Profile Data• Identity Data• Communication Data• Data and Usage Data• Technical Data• Marketing and Communications Data	<ul style="list-style-type: none">• Contractual Obligation• Legitimate Interests (i), (ii), (iv), (v), (vii), (viii) and (ix)• Legal Obligation
To train our employees	<ul style="list-style-type: none">• Communication Data	<ul style="list-style-type: none">• Legitimate Interests (i), (ii), (iii), (iv) and (x)• Legal Obligation

To prevent, detect and investigate potentially prohibited or illegal activities and enforce our legal rights including fraudulent activity	<ul style="list-style-type: none"> • Contact Data • Profile Data • Identity Data 	<ul style="list-style-type: none"> • Legitimate Interests (i) and (iv) • Legal Obligation
To assist in cyber security incident response management	<ul style="list-style-type: none"> • All Data 	<ul style="list-style-type: none"> • Contractual Obligation • Legitimate Interest
To assist to investigate and resolve customer complaints	<ul style="list-style-type: none"> • Contact Data • Communications Data • Identity Data • Incident data 	<ul style="list-style-type: none"> • Legitimate Interest (i), (ii), (iii)
To assist in Legal Proceedings	<ul style="list-style-type: none"> • Identity Data • Contact Data 	<ul style="list-style-type: none"> • Legal Obligation
To assist in dealing with accidents/incidents and providing medical assistance	<ul style="list-style-type: none"> • Identity Data • Contact Data 	<ul style="list-style-type: none"> • Legal Obligation

SPECIAL CATEGORIES OF DATA

We may also collect details about your race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, data about your health and genetic and biometric data. Under UK law, these are called special categories of personal data and require higher levels of protection. We do not seek to collect or otherwise process your Special Category Data, except where:

- we have obtained your explicit consent prior to processing this data
- the processing is necessary for compliance with a legal obligation;
- the processing is necessary for reasons of substantial public interest and occurs on the basis of an applicable law;
- the processing is necessary for the detection or prevention of crime or the establishment, exercise or defence of legal rights.

SHARING OR DISCLOSURE OF YOUR DATA

Except as expressly set out in this Privacy Notice , we do not share, sell, or lease your personal data to any third-parties. We also will never share your personal data with any third parties for the purposes of direct marketing.

In general, we may disclose your personal data to provide our services, respond to legal requirements, enforce our policies and protect our rights and property. The personal data you provide to us may also be shared with affiliated companies if this is necessary to provide you with our services, respond to your inquiries or for any other related purposes.

More specifically:

- We use data processors to provide or assist with some of our services, for example, the processing of ticket purchases. Where we do so, they must agree to strict contractual terms and to keep your data secure;
- Where we share data with other members of the Abellio or Serco Group, this is only in accordance with a written data sharing agreement. Please see Abellio UK's Privacy Notice [here](#) and Serco Privacy Notice here [INSERT LINK].
- To respond to your complaints or administer requests you have made, either to us or another regulatory body such as Merseytravel and the Department for Transport;
- To process payment card transactions;
- To comply with the police or other law enforcement agencies for the purposes of crime prevention or detection, these are dealt with on a case-by-case basis to ensure that any disclosure is lawful;
- To comply with other legal obligations for example, relating to crime and taxation purposes or regulatory activity; and
- To protect our legitimate business interests, as outlined above.
- We share data with our client for the purposes of assisting in the fulfilment of the Contracted Services (Concession Agreement)

Please be assured that we will only share or disclose your data as set out in this Privacy Notice or where the law requires it. However, due to the nature of the services we provide, we process a large range of data, in a number of ways, across a number of solutions. Accordingly, it is not possible to set out the details of all the third parties that we may share your personal data with below. However, we would be more than happy to provide this information to you if you wish to see it. Please just send us an email using the contact details set out below.

Information for Data Subjects in the EEA or UK

If you are based in the United Kingdom ("**UK**") or European Economic Area ("**EEA**"), we may transfer your personal data outside of the UK or EEA to a jurisdiction that does not provide protection of personal data that is essentially equivalent to that which is provided under the applicable law of the UK or EEA. We will only do so, however, for the purposes which we have described in this Privacy Notice .

When we, or our permitted third parties, transfer your data outside the UK or EEA, we or they will impose contractual obligations on the recipients of that data to protect your data 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 data outside of the UK or EEA where: (i) the transfer is to a country deemed by the UK Government or European Commission to provide adequate protection of your data; (ii) where you have consented to the transfer; or (iii) where such transfer is otherwise permissible under Data Protection Legislation (for example where we are required to provide such data 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 and or other regulatory bodies 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).

DATA SECURITY

We have put in place appropriate security measures to prevent your personal data from being accidentally being lost, used or accessed in an authorised way, altered or disclosed.

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 data from unauthorised or inappropriate access, the transmission of data via the internet is not completely secure and we cannot guarantee the security of your personal Data transmitted to us or provided through our Website or Apps. Personal data 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 we collect personal data about you through the use of our Website, Apps or Wi-Fi we will only retain that data for as long as is reasonably necessary to fulfil the activity requested, or as may be required by law.

YOUR RIGHTS

Under certain circumstances, you have rights under data protection laws in relation to your personal data. If you wish to exercise any of the rights set out below, please contact us using the details below. A summary of the rights you have is set out below:

- be informed about the processing of your personal data (i.e. for what purposes, what types, to what recipients it is disclosed, storage periods, confirmation of whether we undertake automated decision-making, including profiling, and the logic, significance and envisaged consequences);
- request access to or a copy of any personal data we hold about you;
- request the rectification of your personal data, if you consider that it is inaccurate;
- request the erasure of your personal data, if you consider that we do not have the right to hold it;
- object to your personal data being processed for a particular purpose or to request that we stop using your data;

- request not to be subject to a decision based on automated processing and to have safeguards put in place if you are being profiled based on your personal data;
- ask us to transfer a copy of your personal data to you or to another service provider or third party where technically feasible; and

ask us to stop or start sending you marketing messages at any time by using the contact details below (See "**Opt Out**")

If you wish to exercise any of these rights, please contact privacy@merseyrail.org

Please see below link for Merseyrail's external Data Subject Request form which will assist you in providing the correct detail required for us to process your request.

https://admin.merseyrail.org/media/3yqd12rd/mel-dsar-form_variant-a-external-2023.docx

HOW WE DEAL WITH RIGHTS REQUESTS

You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive, or excessive. Alternatively, we may refuse to comply with your request in these circumstances.

We may need to request specific data from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further data in relation to your request to speed up our response.

We try to respond to all legitimate requests within one month. Occasionally it may take us longer than a month if your request is particularly complex or you have made several requests. In this case, we will notify you and keep you updated.

There are some limitations and exemptions in relation to the exercise of rights - for example if it would affect another's rights and freedoms or if we need to retain the data 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.

COMPLAINTS

You always have the right to make a complaint to the Data Commissioner's Office ("**ICO**") if you think your data is being misused. The ICO is the UK's supervisory authority for data protection issues (<https://www.ico.org.uk>). (<https://www.ico.org.uk>)

We always appreciate the chance to try to deal with any data protection concerns before they are referred to the ICO so, if you are happy to do so, please do not hesitate to contact us using the details above so that we can try to help you out in the first instance.

Their contact details are: 0303 123 1113 (local rate) or <https://ico.org.uk/global/contact-us/>

HOW LONG DO WE KEEP YOUR PERSONAL DATA FOR?

We'll store your data for as long as we have to by law or regulatory requirement. If there's no legal or regulatory requirement, we'll only store it for as long as we need it. We'll also keep some personal data for a reasonable period after your last contact with us – just in case you decide to use our services again. We, or one of our partners, may contact you about our services during this time if you haven't opted out of receiving marketing communications from us.

We may also keep your personal data for the purposes of our legitimate interests in running our business, including anonymising or pseudonymising data for analysis.

OPT-OUT

If you provide us with personal Data, you may be given a choice at the time to "opt out" of certain uses of that Data (such as sending you newsletters, updated Data about us, our services and offers) by checking or un-checking (as directed) the relevant box.

You also have the option of "unsubscribing" from our mailing list for newsletters, alerts and updates at any time, thereby disabling any further such e-mail communication from being sent to you. To unsubscribe just follow the link within the email. In addition, each electronic mailing we send you will contain details of how you can unsubscribe.

Please note that it may take up to 28 days to action your request.

CHANGES TO THIS PRIVACY NOTICE

Any changes we may make to our Privacy Notice

in the future will be posted on this page. We recommend that check this page from time to time to take notice of any changes we make,

This Notice was last updated in March 2023.