Privacy Notice

1. About this privacy notice

C2C Railway Limited ("C2C", "we", "us" or "our") takes your privacy seriously. We want to be open and honest about how we handle your personal information and make sure you understand what we do with it.

This Privacy Notice explains:

- What personal information we collect and how we use it
- Why we're allowed to use your personal information (this is called our "lawful basis")
- What your rights are under data protection law and how you can exercise them
- How you can control the way we use your personal information

C2C operates train services between London Fenchurch Street, Basildon, Grays, Shoeburyness and surrounding areas. Our full company name is C2C Railway Limited, and we're registered with the UK's data protection regulator – the Information Commissioner's Office (ICO).

ICO registration number: ZB549466

This privacy notice applies to the personal information we collect about you when you use our services, including through our websites (https://www.c2c-online.co.uk/ and tickets.c2c-online.co.uk), mobile apps, social media, by phone, by post, in person at our stations or on board our trains, and when you otherwise communicate with us.

We may update this notice from time to time, and the most up-to-date version will always be available on our website. We'll also let you know if we make any major changes.

If you have any questions or want to exercise your rights, you can contact our Data Protection Officer at: **dpo@c2crail.net**.

2. What is Personal Data

"Personal data" (or "personal information") means anything that can identify you. This includes things like:

- Your name, address, phone number, or email address.
- Your payment details when you buy tickets from us.
- Information about how you use our website or travel on our trains.

If information can be linked to you, it's classed as personal data.

3. What does 'processing' mean?

When we process personal data, we mean anything we do with it - such as collecting, storing, using, or sharing it. For example, when you buy a ticket online, we collect your name and payment details, store them securely, and use them to issue your ticket and send you a confirmation email.

4. Who decides how your data is used?

C2C is the "data controller". This means we are responsible for deciding how and why we use your personal data.
We follow the rules set out in:

- **The UK General Data Protection Regulation (UK GDPR)** – This is the main law that protects how your personal data is collected, used, and shared.
- **The Data Protection Act 2018 (DPA 2018)** – This law works alongside UK GDPR and sets out extra rules, such as how data protection applies to law enforcement and national security.
- **The Privacy and Electronic Communications Regulations (PECR)** – These rules cover things like marketing emails, cookies, and how we contact you electronically.
- **The Data Use and Access Act 2025 (DUAA 2025) –** This sets out additional rules about how organisations access, share and use personal data, especially across public services.

These laws mean we have to use your data fairly, lawfully, and transparently.

5. How to contact us about your personal data

If you have any questions about how we use your data or if you want to exercise your rights (which we explain later in this notice), you can contact us in the following ways:

Email: dpo@c2crail.net,
Website Portal: **DPO Web Portal**
Phone: 0330 109 8130
Post: DPO, c2c, 7th Floor, Centennium House, 100 Lower Thames Street, London EC3R 6DL

6. Where and How We Collect Your Personal Information

We collect personal information from different sources, including directly from you, from devices you use, from public sources, and from other organisations.

1. Information you give us directly

We collect personal information when you:

- Fill in a form on our website or mobile app, or contact us by phone, email, or other methods.
- Register for an account on our website or app, including signing in via a social media account.
- Subscribe to our services, such as ticket alerts or newsletters.
- Purchase something from us, including train tickets.
- Choose to receive marketing messages by email, post, SMS, or other means.
- Register to use our onboard or station Wi-Fi.
- Enter a competition, promotion, or fill in a survey run by us or on our behalf.
- Use our website, mobile app, or open our emails or push notifications.
- Call our customer service team – We record calls for training, quality, and security purposes.

2. Information we collect automatically

When you use our website, app, or onboard/station Wi-Fi, we automatically collect information from your device. This may include:

- Device type and settings
- IP address
- Location data (if you allow this on your device)
- Browsing behaviour (such as pages visited or links clicked)

See the next section for more details on how we collect and use website and Wi-Fi data.

3. Information from CCTV and body-worn cameras

We use CCTV cameras on our trains and at stations, as well as body-worn cameras worn by staff, to:

- Ensure safety and security.
- Prevent and investigate incidents.
- Support revenue protection activities.

Body-worn cameras record audio and video and are used in situations such as fare disputes or anti-social behaviour.

4. Information from other organisations

We may receive personal information about you from:

- Law enforcement agencies (e.g., the police or British Transport Police) in relation to incidents, investigations, or security concerns.
- Rail station operators if an incident involving you takes place at a station where we operate.
- Other Train Operating Companies (TOCs) if required for fraud prevention or revenue protection.
- Credit reference agencies or fraud prevention databases if we need to verify information as part of fraud prevention or security checks.

5. Revenue protection and fraud prevention

We process information we hold about you to detect, investigate, and prevent fare evasion or other fraudulent activity. These measures help ensure fair travel for everyone and protect our services from misuse. Where required or permitted by law, we may share relevant data with law enforcement agencies, other train operators, or carefully chosen third parties.

This processing is carried out in line with our statutory and contractual obligations (including the Regulation of Railways Act 1889 and Railway Byelaws) and under Schedule 2, Part 1 of the Data Protection Act 2018, which permits the use of personal data for the prevention or detection of crime.

Because this processing is necessary for the performance of a public task in the public interest, you do not have the right to object under Article 21(6) of the UK GDPR. However, if a fraud investigation directly affects you, you can contact us for more information on how your data was used.

7. What Personal Information Do We Hold About You?

We collect and use different types of personal information depending on how you interact with us. This includes:

Contact and Payment Information

When you fill in a form, buy a ticket, or create an account, we collect:

- Your name, address, phone number, and email address.
- Your payment details (e.g. bank or credit card information) for ticket purchases or other transactions.
- Your communication preferences (e.g. how you'd like to hear from us).

User Information

This is information we collect about you as a customer using our services:

- **Address & travel history** – If you've entered your address in your C2C account, we may use this along with your ticket purchase data to understand how far people travel to our stations.
- **Competitions and prize draws** – If you enter a competition, we collect the personal details needed to manage the entry, such as your name, age (if required), and contact details.
- **Customer feedback and research** – We collect opinions from people who take part in:
  - Forums and opinion panels
  - Accessibility groups (to improve services for passengers with additional needs)
  - Customer satisfaction surveys

Special Category & Criminal Offence Data ("Sensitive Information")

In some cases, we may need to process confidential or sensitive information about you. For example:

- **Passenger assistance** – If you need help boarding or leaving a train, you may provide details of a medical condition or mobility requirements. We use a system called Passenger Assist to ensure staff know how to help you.
- **Incidents & investigations** – If you commit, are suspected of committing, or are a victim of fraud or another crime, we may process data related to this. This could include information from ticket inspections, delay repay claims, or incidents on our trains or at stations.

Website and Wi-Fi Information

When you use our website, mobile app, or onboard Wi-Fi, we automatically collect:

- **Technical details** – IP address, browser type, operating system, and train location (if using onboard Wi-Fi).
- **Usage data** – Pages you visit, how long you stay on them, what you click on, and how you navigate our site.
- **Location data** – If you enable location services on your device.

Marketing and Communication Data

We also track how you interact with our emails, SMS, and push notifications, including:

- Which emails you open and click on.
- Your device type and model.
- Your approximate location when you engage with our messages.

We use cookies and tracking technologies for marketing and advertising purposes. Where required by law, we seek your consent before setting these cookies.

For more details on how we use cookies and how to manage your settings, see our **section on Cookies**.

Inferred Data and Segmentation

Sometimes, we make reasonable assumptions based on the data we already hold. For example:

- If you regularly buy children's tickets, we may infer that you are a parent or guardian.
- If you travel frequently between the same locations, we may assume you are a commuter.

These insights are useful for us as a business and service provider because they allow us to:

- Improve our services – Understanding travel patterns helps us plan for demand, enhance customer experience, and develop new offers that suit different types of travellers.
- Make our communications more relevant – By grouping customers into broad categories (such as "commuters" or "families"), we can send information about offers or services that are more likely to be of interest to you.

We may analyse customer data to create groups based on travel habits (e.g., commuters, families) to improve our marketing and services. We may also use certain patterns or behaviours (such as unusual travel activity) as part of our wider efforts to detect and prevent fraud.

We do not make automated decisions that have a legal or similarly significant effect on you, unless we've told you about it elsewhere in this notice (for example, in relation to Delay Repay claims, which you can appeal).

Information from Other Sources

Sometimes, we receive data about you from third parties, including:

- Law enforcement agencies (e.g. police, British Transport Police) in relation to incidents or investigations.
- Other Train Operating Companies (TOCs) – TOCs may share or request information from us for fraud prevention, revenue protection, or in relation to accidents or incidents on the railway. This could include ticketing data, accident details, or CCTV footage where appropriate.
- Rail station operators if an incident involving you occurs at a station where we operate.
- Credit reference agencies or fraud prevention databases if we need to verify your details for security or fraud checks.

CCTV & Body-Worn Camera Footage

We use CCTV cameras on our trains and at stations, as well as body-worn cameras worn by staff, to:

- Prevent and detect crime.
- Investigate incidents on our trains or in stations.
- Provide evidence for legal or safety-related investigations.
- Ensure safety for passengers and staff.

We keep CCTV footage for 30 days or less, unless required for an ongoing investigation or by law.

Accessing CCTV Footage

You have the right to request a copy of CCTV footage of yourself (this is called a Data Subject Access Request). To do this, contact our Data Protection team.

However, the right of access is not a blanket right, and we must balance your request against other legal considerations, including:

- The rights and freedoms of others – We cannot provide footage that includes other identifiable people unless their privacy can be protected.
- Whether the request is reasonable – If a request is manifestly unfounded or excessive, we may refuse it.
- The effort involved in retrieving footage – Extracting CCTV footage is a complex process, and we prioritise requests from law enforcement agencies before others.

Police Requests

We will process police requests for CCTV footage when they make an enquiry about theft or other criminal incidents that have taken place on our trains or at our stations. Police requests are prioritised over other types of requests.

Car Park Incidents

If your car has been damaged in one of our managed car parks and you need CCTV footage, please note:

- We will not provide footage directly to you. Your insurer must request it on your behalf.
- You can still contact us first. Insurers can take a long time to process requests, so it's best to check with us before they make a formal request.
- Be realistic about timeframes. If your car was parked for a significant period, it is highly unlikely we will review the footage. CCTV must be watched in real-time, and we do not have the resources to review days' worth of footage manually.

Examples of Disproportionate or Unreasonable Requests

Some requests may be deemed disproportionate, meaning that the effort required to fulfil them outweighs their necessity or benefit. Examples include:

- **Requesting CCTV footage of a suitcase** – Under data protection law, CCTV only applies to identifiable, living individuals, so we cannot provide footage of objects such as suitcases. However, if the police request the footage as part of an investigation, we will cooperate and provide it to them where appropriate.
  Requesting footage as proof for a delay repay claim We will not provide CCTV footage to show that you were on a train, as this is not required to assess Delay Repay claims and would be a disproportionate use of resources. There are other ways to confirm whether a train was late or on time, and we will provide this information through appropriate channels.
  Requesting several days' worth of car park footage – We do not have the capacity to manually review this amount of footage in real-time.

When Might We Refuse a Request?

We may decline a request if:

- The request was made with malicious intent, submitted in bad faith or intended to cause disruption. We would refer to this as manifestly unfounded.
- Providing the footage would place an undue burden on C2C.
- The request is not valid under UK GDPR (e.g., asking for footage of an object or something that does not contain your personal data).
- It is impossible to extract or edit the footage without breaching the privacy of others.

Sharing CCTV with Law Enforcement

We may share CCTV footage with law enforcement agencies (e.g., the police, British Transport Police) when required for criminal investigations, safety concerns, or legal matters. Police requests are prioritised over public requests due to their importance in maintaining security and enforcing the law.

8. Our Lawful Basis for Using Your Personal Information

Under UK data protection law, we must have a valid reason (known as a "lawful basis") for collecting, storing, and using your personal data. The basis depends on what we're using your data for. These are the lawful bases we rely on:

1. **Fulfilling a contract** – We need your data to provide the service you have requested.
   Example: When you buy a train ticket, we collect your payment details and email to process the transaction and send your ticket.

2. **Consent** – You have actively agreed to us using your data for a specific purpose.
   Example: If you opt in to receive marketing emails, we rely on your consent to send them. You can withdraw consent at any time for things like marketing. However, if consent was not the original basis for processing your data, there is nothing to withdraw.

3. **Legitimate interests** – We have a business reason to use your data, as long as it does not override your rights.
   Example: We may analyse travel patterns to improve services or share passenger data with a new train operator when a franchise changes.

4. **Legal obligation** – We must process your data to comply with the law.
   Example: Keeping financial records for tax purposes or sharing data for fraud prevention.

5. **Vital interests** – We need to process your data to protect life or safety.
   Example: If you become seriously unwell on a train, we may share relevant medical details with emergency services.

6. **Substantial public interest** – We use your data for matters that serve the public good.
   Example: Investigating fraud or criminal activity.

7. **Explicit consent** – In some cases, we need your clear and specific agreement to process sensitive personal data.
   Example: If you use Passenger Assist, we may store details of your mobility requirements, but you can remove or update this at any time.

Important: You can't withdraw consent if it wasn't the basis we relied on – for instance, when we process your data to deliver a ticket, that's done under a contract, not consent.

9. For what purposes do we use your personal information

We use your personal information for different purposes depending on the service. In most cases, we rely on the lawful bases of contract, legal obligation, consent (where needed), or our legitimate interests. Where we're delivering services under direction from the Department for Transport, some processing may also be considered a public task carried out in the public interest. If that applies, we'll only rely on it where we believe it's legally justified.

Providing Services & Fulfilling Your Requests

We process your data to:

- Respond to enquiries and complaints.
- Fulfil the service or information you have requested, such as issuing tickets and confirming orders.
- Administer payments and manage purchases.
- Provide post-sales support, including refunds, complaints, and ticketing or travel issues.

Lawful Basis: Contract (where necessary to provide services) or Legitimate Interests (for general support and service improvements).

Communicating With You

We may use your information to:

- Send essential service communications, such as updates about your booked journey.
- Notify you when tickets for your journey go on sale.
- Inform you of updates to this Privacy Notice and any changes to how we process your data.

Lawful Basis: Contract (for service updates) or Legitimate Interests (for notice updates and operational messages).

Marketing & Personalisation

Where permitted, we use your data to:

- Send marketing messages about offers and relevant travel suggestions.
- Personalise your website experience by making recommendations based on your purchases and browsing activity.
- Analyse and optimise our marketing activities, including market research and surveys.

Lawful Basis: Consent (for marketing) or Legitimate Interests (for website personalisation and marketing analysis).

Wi-Fi & Technical Support

If you use our Wi-Fi, we may process your data to

- Provide the service, including collecting technical information from your device (such as device ID, connection status, and usage data)

- Assist you with technical issues through our helpdesk.

Lawful Basis: Contract (if Wi-Fi is part of your ticketed service) or Legitimate Interests (for operational support).

Safety, Security & Law Enforcement
We may process personal data to:

- Help you in an emergency situation, such as via Passenger Assist.
- Handle law enforcement requests for CCTV footage.
- Support investigations into crimes or serious incidents on our trains or at our stations.

Lawful Basis: Vital Interests (for emergencies), Legal Obligation (where required by law), or Legitimate Interests (for security purposes).

Below, we explain these purposes in more detail, along with the Lawful Basis we rely on under data protection laws

When do we rely on your consent?
We only use your personal information based on your consent in specific situations. Below is an overview of when we rely on consent and what it covers. You can withdraw your consent at any time.

Purpose of Processing	When We Rely on Your Consent
Sending you marketing communications (including offers, service updates, and promotions)	We only send direct marketing if you've opted in.
Journey alerts and ticket sale notifications	We send these when you've asked to receive them – for example, alerts for a specific route.
Sharing data with partner services or platforms (e.g. social media tools, referral schemes)	We only ask for your consent if required by law or where the third party will use your data for their own purposes.

When we process your data to perform a contract
We use your data when it is necessary to fulfil a contract with you, such as providing a service you have requested.

Purpose of Processing	Why This Applies
Responding to your enquiries and complaints	We need to respond to customer requests as part of our service commitment.
Fulfilling the service or providing the information you've requested	This is necessary to deliver the services you have requested.
Handling the administration of your payment, issuing tickets/products, or confirming orders	We need to process transactions and issue tickets or confirmations.
Providing post-sales support (e.g. complaints, refunds, ticketing or travel issues)	This ensures you receive support for any issues related to your purchase.
General record-keeping and passenger relationship management	We maintain records to manage our customer relationships.

When we process your data to comply with a legal obligation
We are required by law to process certain types of data, including for safety, security, and regulatory purposes.

Purpose of Processing	Why This Applies
Contacting you about updates to this Privacy Notice or changes to data processing	We are legally required to inform you of significant notice changes.
Using CCTV on our trains and in stations to prevent, deter, and detect crime	We have a legal duty to ensure safety and security on our trains and at stations.
Providing CCTV footage to law enforcement agencies	We may be required by law to share CCTV in response to a court order or police investigation.
Establishing and enforcing our legal rights	We must take action to protect our business operations and customers.
Complying with requests from law enforcement agencies, courts, or regulators	We are required to share certain information as mandated by law.
Managing a sale, restructuring, or merger of our business	We must follow legal requirements in corporate transactions.
Keeping records to comply with tax, consumer protection, and data protection laws	We have legal obligations to retain records for regulatory purposes.

When we process your data for our legitimate interests
In some cases, we process your personal data because it is necessary for our business operations, provided it does not override your rights.

Purpose of Processing	Why This Applies
Responding to enquiries, complaints, and post-sales support (e.g. refunds, ticketing issues)	It is in our interest to provide good customer service and ensure customer satisfaction.
Fulfilling the service or providing requested information	We must provide accurate and timely service to customers.
Handling the administration of payments, issuing tickets, or confirming orders	Ensuring smooth transactions is essential to our service.
Sending service communications (e.g. ticket confirmations, updates, journey alerts)	Keeping customers informed about their travel plans is part of our engagement with them.
Personalising your website experience (e.g. recommending relevant services)	Enhancing the customer experience makes our service more useful.
Improving our website, services, and products	Continuous improvements help us better meet customer needs.
Conducting market research and surveys, analysing marketing activities	Gathering feedback allows us to refine our services and better engage with customers.
Assisting with Wi-Fi technical support and ensuring website functionality	Ensuring reliable digital services benefits customers.
Using CCTV to prevent, deter, and investigate crime	CCTV helps maintain security and supports law enforcement.

10. Automated decisions (e.g. Delay Repay)

We use automated tools to decide the outcome of Delay Repay claims. These help us process claims fairly and quickly by assessing eligibility and calculating any compensation due.

If you disagree with an outcome, you can appeal. Some appeals are reviewed automatically again, and others are passed to our team for a manual check. If you're still not happy after this, you can ask Customer Relations to look into it further.
We don't make automated decisions with legal or similarly significant effects unless there's a route for a human to step in and review the outcome.

11. Aggregated and Anonymised data

We sometimes use your information in an aggregated form, where all personally identifiable details are removed. Once data is fully anonymised, it is no longer considered personal data under data protection law.
However, the process of anonymising data itself does fall under UK GDPR, which means we must ensure that personal data is handled securely and lawfully before we remove any identifiable details.
Why do we do this?

- To support marketing and strategic development, helping us improve and sustain our business.
- To conduct research and analysis, including producing statistical reports that guide our business decisions.

For example, we might analyse anonymised travel patterns to understand which routes are most popular or identify potential target markets for new services.
How does this protect your data?

- By converting your personal information into a statistical or aggregated form, we ensure that your identity is protected.
- Anonymised data cannot be linked back to you, safeguarding your data even as we use insights for business development.

Lawful Basis: The process of anonymisation falls under UK GDPR, as we must handle your data lawfully before making it non-identifiable. However, once anonymised, the data is no longer subject to data protection laws because it can no longer be linked to you.

12. When we process your special category or sensitive data

When we refer to "sensitive information", we mean special category data (such as health information) and criminal conviction or offence data, as defined under data protection law.
We understand that some types of personal data, such as bank account details or payment information, may feel sensitive. However, these are not classified as "sensitive information" under data protection law - they are still protected, but they do not require the same legal justifications as special category or criminal offence data.
There may be situations where the examples below do not involve sensitive information - for instance, general CCTV monitoring or processing standard personal data for customer service purposes. However, this table only applies when the processing involves special category or criminal offence data.

Purpose of Processing	Explicit Consent	Vital Interests (where consent cannot be given)	Legal Claims	Substantial Public Interest

Helping you in an emergency situation		✓		✓
Providing Passenger Assist services	✓			✓
Responding to law enforcement agency requests for CCTV (where the footage is used in relation to a crime or criminal investigation)				✓
Dealing with fraud, crime, or serious incidents on our trains or at railway stations, including fraud involving delay repay claims or suspicious ticket purchases			✓	✓

13. How we use your personal information for marketing

We use your personal information to develop, analyse, and optimise our marketing activities, including sharing travel offers, ideas, and news with you.

How We Send Marketing Communications

We may contact you through:

- Post, email, phone, SMS, social media, or digital advertising (such as Google and Facebook).
- Personalised marketing messages based on your online activity and past interactions with us.

For example, we may use your name, address, location, and past journeys to ensure our marketing is relevant, accurate, and effective. We also use tools like Google and Facebook to target you with personalised messages based on your online behaviour.

Lawful Basis for Marketing

We only send marketing messages where we have:

- Your consent (e.g., when you opt in to receive marketing emails).
- A legitimate interest (e.g., where we have a commercial reason to contact you, but we ensure this does not override your rights).

We also use your information to create a personalised experience on our website and to show you offers or rewards that are relevant to you.

How to Opt Out of Marketing

You can opt out of marketing at any time by:

- Clicking the "unsubscribe" link in our marketing emails.

- Replying "STOP" to a marketing text message (this will not stop essential service updates, such as ticket confirmations).
- Logging into your C2C account and updating your marketing preferences.
- Contacting our Data Protection team by email, phone, or post.

Important: Even if you opt out of marketing, you will still receive service communications, such as booking confirmations, disruption notices, and timetable changes.

14. Who else might we share your personal data with

We share your personal information with third parties for various reasons, including business operations, service delivery, and legal requirements.

1. Third parties acting as our data processors

Some third parties carry out business functions on our behalf, such as website administration, IT support, and payment processing. These companies act as data processors under data protection law, meaning they only process your personal data based on our instructions.
We ensure these third parties have appropriate security standards in place before sharing any personal data. Examples include:

- IT service providers supporting website maintenance, software, data hosting, and backups.
- Payment processors handling card payments for ticket purchases.
- Mailing houses sending pre-booked tickets.
- Wi-Fi suppliers supporting onboard internet services.
- Customer service providers assisting with ticketing, complaints, and other passenger services.

2. Third parties acting as independent data controllers

In some cases, we share your personal data with third parties who act as data controllers in their own right. This means they make their own decisions about how to process your data. We may share data in the following circumstances:

- **Rail franchise transition.** If another company takes over the C2C franchise, we may share your data with the new operator to ensure service continuity. They must process your data lawfully and in line with this Privacy Notice.
- **Business sale or restructuring.** If C2C is sold or merged, we may transfer your personal data to the new owner or their advisors.
- **Legal and regulatory requirements**. We may disclose personal data to comply with legal obligations, enforce contracts, or protect the safety and rights of customers, employees, and others.

3. Categories of recipients we share data with

Business and service providers

- Replacement operator of the rail franchise
- IT support, data hosting, and system administrators
- Ticketing and payment service providers

- Mailing houses sending pre-booked tickets and marketing materials
- Website developers and hosting providers managing website content and personalised messaging
- Wi-Fi providers supporting onboard internet services
- Website analytics and customer research agencies
- Customer service agencies supporting rail staff

Marketing and advertising partners

- Email service providers sending marketing emails
- Mailing houses distributing marketing materials by post
- Telemarketing agencies contacting customers via phone or SMS
- Online advertisers such as Google and Facebook delivering and tracking digital marketing campaigns
- We may share hashed first-party data (such as your email address) with Google to help measure the effectiveness of our advertising campaigns through Enhanced Conversions.
- We may also share your data with advertising platforms (such as Sky Media) to create "lookalike audiences". These platforms match our customer data with their own to find people with similar characteristics or behaviours. This helps us show relevant adverts to potential new customers. The platform deletes our data after use and isn't allowed to use it for any other purpose.

Legal, regulatory, and insurance-related third parties

- Legal and professional advisors, including lawyers and accountants
- Courts, appointed representatives, and insolvency practitioners
- Business partners and joint ventures
- Insurers
- Government and regulatory bodies, including the Department for Work & Pensions, Financial Conduct Authority, Information Commissioner's Office, HMRC, and the police

4. How we protect your data when sharing it

All personal information shared with third parties is transferred securely. When third parties act as data processors, they:

- Must comply with our instructions and cannot use your data for their own business purposes.
- Must have technical and organisational measures in place to protect your data.

For independent data controllers, we only share what is necessary and ensure they comply with data protection laws.

15. Future of the railway and your data

C2C is currently operated under public ownership by a government-owned company called the Department for Transport Operator (DFTO). The DFTO acts as the commercial arm of the Department for Transport.

If the legal company running C2C changes in future (for example, if a different DFTO company is appointed), your personal data may be transferred to that new company. This helps ensure continuity of service – including your bookings, customer service history, and, where applicable, your marketing preferences.

If you've opted in to receive marketing communications, those preferences would carry over so you don't miss out on updates or offers you've asked for. You can still change or withdraw your preferences at any time.

If this kind of change happens, we'll update this Privacy Notice to explain who the new data controller is. Your data protection rights won't change, and you'll be able to contact the new controller with any questions or concerns.

16. Where is your personal information stored?

We aim to keep as much of your personal data as possible within the UK and the European Economic Area (EEA). In fact, this is something we take very seriously and actively work to achieve. However, in some cases, we may need to transfer your data outside these areas if there is no practical alternative.

Some countries already have data protection laws equivalent to those in the UK and EEA, but where this is not the case, we ensure that appropriate safeguards are in place. These safeguards may include:

- **Contractual obligations** – We require recipients to sign legally binding contracts to protect your data to UK and EEA standards.
- **International frameworks** – Where relevant, we use recognised frameworks that support secure cross-border data sharing.

If you would like more information about the safeguards in place, or details on where they are available, you can call, email, or write to our Data Protection team.

17. Your data protection rights

Your personal information is protected under data protection law, and you have specific rights. These don't apply in all situations, but if you ask to use a right, we'll always explain whether it applies and why.

- **The right to be informed** – You have the right to know how we use your data. That's why we have this Privacy Notice.
- **The right to correct inaccurate information** – If your details are wrong, you can ask us to fix them. You may also be able to add missing information.
- **The right to object to processing** – You can object to us using your data in certain cases:
    - When we rely on legitimate interests (unless we have a compelling reason to continue)
    - For *direct marketing* – you can always opt out
    - For statistical research, in some circumstances

- **The right to restrict processing** – You can ask us to limit how we use your data:
- **The right to erasure ("right to be forgotten")** – You can ask us to delete your data in some situations:
    - If it's no longer needed for its original purpose
    - If you withdraw consent (and consent was the legal basis)
    - If it was processed unlawfully
    - If we're legally required to delete it

We may refuse erasure if we need to keep the data for legal, contractual, or regulatory reasons, or to establish or defend legal claims.
If you later provide your data to us again (e.g. by signing up to marketing), we'll treat you as a new customer.

- **The right of access ("subject access request")** – You can ask us:
    - Whether we hold your data
    - For a copy of your data
    - How we use it (although this Privacy Notice covers most of that)

- **The right to data portability** – If we process your data under consent or contract and use automated systems, you can ask us to move it to another provider. This right is limited and unlikely to apply to most of our services.
- **Rights relating to automated decisions and profiling** – If a decision with significant impact is made by automated means only (without any human involvement), you can request a human review and challenge the decision.
- **The right to complain to the ICO** – If you're unhappy with how we've handled your data, you can contact the Information Commissioner's Office: https://ico.org.uk

If you'd like to know more about your rights or want to use any of them, please contact our Data Protection team at **dpo@c2crail.net**.

18. Accessing your data (Subject Access Request – SAR)

You have the right to ask for a copy of the personal information we hold about you. This is called a Subject Access Request (SAR).
We provide this information free of charge, except in limited cases—for example, repeat or clearly unreasonable requests. We aim to respond within one month of confirming your identity.
If your request is very broad or complex and can't be completed within a month, we will:

- Send you the information we can within the deadline
- Keep you updated on our progress

- Provide the rest as soon as possible, in line with UK data protection law and ICO guidance

If you'd like a copy of your personal data, please email or write to our Data Protection team. Unless you ask for a different format, we'll usually provide the data electronically - especially if your request was made by email or social media.
We may ask you to narrow down your request if:

- It's too broad to process reasonably
- It looks like you're trying to find something specific, and narrowing the scope will help us locate it faster

If we ask for clarification, we'll explain why and help you refine your request so you get what you need as quickly as possible.

If we hold personal data about you, we'll:

- Describe the data we hold
- Explain why we're processing it
- Say who it may be shared with
- Tell you how long we'll keep it
- Let you know where we got it (if not from you)
- Say whether it's been used for automated decisions
- Confirm if it's stored outside the UK or EEA, and what safeguards apply
- Give you a clear, concise copy of the data

Requests for CCTV Footage

You can request CCTV footage of yourself as part of a Data Subject Access Request (DSAR), but there are limits on when we can provide it.
Please see the *CCTV and body-worn camera* section of this Privacy Notice for more detail. That section explains:

- When we can share footage with you
- What legal and technical limits apply
- Why we may need to prioritise law enforcement requests or protect the privacy of others

19. How we keep your personal information up to date

We have a legal duty to keep the personal information we collect accurate and up to date. You have the right to ask us to correct anything that's inaccurate, and to restrict how we use your data until it's been corrected.
The easiest way to keep your information accurate is to log into your account on our website and update your details. You can also contact our Data Protection team to make changes.
We help keep your data accurate by:

- Giving you the opportunity to update your information at any time
- Asking you to confirm details when you contact us
- Updating our records when we receive undelivered mail or email

20. Keeping Your Personal Information Accurate and Secure

We have a legal obligation to keep your personal information accurate and up to date. You also have the right to ask us to correct any inaccuracies, and to restrict how we use your data until it's been corrected.
The easiest way to keep your details accurate is to log into your account on our website and update them directly. You can also contact our Data Protection team to request updates.

We help maintain accuracy by:

- Letting you update your details at any time
- Asking you to confirm key details when you get in touch
- Updating our records when we receive undelivered mail or email

We also use a combination of administrative, electronic, and physical safeguards to protect your data from:

- Unauthorised access
- Unlawful processing
- Accidental loss, destruction or damage

21. How Long We Keep Your Personal Information

We retain your personal information only as long as necessary for the purposes outlined in this Privacy Notice. This includes:

- Fulfilling the purpose for which the data was collected.
- Complying with legal and regulatory requirements.

- Retaining it for claims, complaints, or disputes.

If you would like more details about our data retention policy, you can contact our Data Protection team.

How We Determine Retention Periods

- **Ticket bookings.** We keep personal data related to your ticket booking until you have completed your journey. We retain it for a necessary period afterward to handle delay repay claims, complaints, or disputes. It is not kept beyond that unless required for other reasons.
- **Claims and disputes.** We keep certain personal information for as long as you may legally bring a claim against us.

Type of data	Retention period
Marketing consent	Needs to be refreshed 24 months after last customer interaction
Customer complaints, compensation claims and investigations	24 months from the date of the incident, unless subject to legal proceedings
Refund cases	12 months
Customer call recordings	No longer than 12 months (unless part of a complaint – see above)
Wi-Fi registration & usage	24 months after last recorded use
My Customer Account (web account, e-ticket/smart ticket account, Goldstar season ticket database)	24 months after last recorded use
Default retention period for all surveillance camera systems	No longer than 30 days
CCTV or BWV footage designated potentially relevant for verification or assist with the verification of criminal investigation/civil claim (insurance and 3rd party claims) or complaint	3.5 years
CCTV or BWV footage chain of custody documentation	3.5 years
CCTV or BWV footage and actual documentation designated as actually relevant for verification or assist with the verification of civil claim (insurance and 3rd party claims) or complaint	7 years
CCTV or BWV footage disclosed following a Subject Access Request	7 years

22. Cookies

The Website uses cookies. Cookies are text files containing small amounts of information which are downloaded to your personal computer, mobile or other device when you visit a website. For more information, please see our **Cookie Notice**.

23. What to Do If You Have a Complaint About Our Use of Your Personal Information

If you have a complaint about how we handle your personal information, please contact our Data Protection team, and we will do our best to resolve your concerns as quickly as possible.
We understand that data protection matters can be important and sometimes frustrating, but we ask that you treat our team with respect. We are here to help, and we will not tolerate abusive or aggressive behaviour.

- Website Portal: **DPO Web Portal**
- Email: **dpo@c2crail.net**
- Phone: 0330 109 8130
- Post: Data Protection Officer, c2c, 7th Floor, Centennium House, 100 Lower Thames Street, London, EC3R 6DL

If you are not satisfied with our response, you have the right to escalate your complaint to the Information Commissioner's Office (ICO). You can find their contact details in the section above or visit www.ico.org.uk for more information.

24. Links to Other Websites

Our website may contain links to external sites, such as the ICO's website referenced in this Privacy Notice. However, this Privacy Notice only applies to C2C and does not cover any third-party websites or organisations we may link to.
We strongly encourage you to read the privacy policies of any external websites you visit to understand how they handle your personal information.

Changes to This Privacy Notice

We review our Privacy Notice regularly to ensure it remains accurate and up to date.

This Privacy Notice was last updated on 20 July 2025.

Cookie Notice

(Posted 13/09/2022)

1. Introduction

We use cookies and similar technologies (such as pixels and beacons) on our websites, mobile app, and Wi-Fi portal to collect information. This includes details about your browsing and purchasing behaviour, such as pages viewed, products purchased, how you move through our site or app, and whether marketing communications are opened.

This Cookie Notice explains what these technologies are, how we use them, and how you can manage your choices. Cookies that are not essential for the operation of our services are only used if you give us permission.

2. What are cookies?

Cookies are small text files that are downloaded to your device (such as a computer, smartphone or tablet) when you visit a website. They're sent back to the same website on later visits, or to another site that recognises the cookie.

Cookies allow a website to recognise your device and support useful features. For example, they can make it easier to log in, remember your preferences, and help you move around the site more smoothly. They also help us understand how people use our site and, if you've given permission, to show you more relevant content and advertising.

Cookies don't give us access to your device or reveal personal information like your name or email address. They only record information about your visit, such as which pages were viewed and for how long.

3. Types of cookies?

We group the cookies we use into the following categories:

Necessary cookies
These are essential for the website to function properly. They enable core features like page navigation, secure log-in and shopping basket functions. These cookies do not require your consent.

Preference cookies *(used only if you consent)*
These remember choices you've made, such as:

- Whether you've completed a survey
- Whether you've visited before
- Your preferred language or region

Statistics cookies *(used only if you consent)*
These help us understand how visitors use our site so we can improve it. For example:

- Tracking which pages or links are used most often

- Identifying navigation patterns
- Diagnosing where error messages may occur

The data is grouped and anonymous. These cookies don't identify individual users.

We use Google Analytics, a service provided by Google LLC, to support this. Google Analytics sets cookies to collect usage information and create reports about how the website is used. This data may be transferred outside the UK or EU, including to the United States. These cookies are only set if you consent via our cookie settings.
You can also opt out globally by visiting Google's opt-out tool.

Marketing cookies *(used only if you consent)*
These track your browsing behaviour and may be used to:

- Show you more relevant ads based on your interests
- Measure how effective a marketing campaign was
- Share data with third-party advertisers or partners

Affiliate cookies *(used only if you consent)*
Some pages may contain links to partner websites. If you click one and go on to register or purchase something, a cookie tells the partner site that you came from us. This may result in us receiving a referral payment. These cookies are also classed as marketing and require your consent.

Other tracking technologies
We sometimes use small files called pixels or web beacons in emails and on our websites to measure engagement. For example, they help us know whether a marketing email has been opened or if a page has been viewed.

4. How do I change my cookie settings?

When you visit our website for the first time, you'll see a cookie banner explaining that we use cookies and why. The banner lets you manage your cookie preferences, including choosing which types of cookies you want to allow.

You can update your cookie preferences at any time by clicking the Cookie Preferences link, which appears in the footer of every page on our website.

Please note: if you disable certain types of cookies (such as Preference or Marketing cookies), some features of the site may not work as intended.

You can also manage cookies using your web browser settings. To find out more about cookies and how to control or delete them, you can visit:

- www.aboutcookies.org
- www.allaboutcookies.org

To manage cookies in common browsers:

- **Google Chrome**
- **Microsoft Edge**
- **Mozilla Firefox**
- **Opera**
- **Apple Safari**

To find information relating to other browsers, visit the browser developer's website.

To opt out of Google Analytics tracking across all websites, visit:
https://tools.google.com/dlpage/gaoptout

End of document.