

FirstGroup – Employee Privacy Notice



This Privacy Notice applies to all employees and workers engaged by FirstGroup plc (or any of its subsidiaries or associated entities) based in the UK and Ireland (**FGUK companies**).

Created: May 2018

Last updated: April 2022

CONTENTS

ABOUT THIS PRIVACY NOTICE

This section explains how we are committed to protecting the privacy and security of your personal data. It also explains how compliance with this Privacy Notice will be monitored.

HOW WILL WE USE YOUR PERSONAL DATA?

This section explains how we will collect, store and use personal data that you provide to us. This is to enable us to carry out our activities and obligations as your employer.

WHO WILL HAVE ACCESS TO YOUR PERSONAL DATA?

This section explains which of our employees will have access to your personal data. It also explains the reason for our employees accessing your personal data.

WHO ELSE MIGHT WE SHARE YOUR PERSONAL DATA WITH?

This section informs you of who we share your personal data with. It also explains the reason for sharing; this is largely so that we can carry out our activities and obligations as your employer.

HOW LONG DO WE KEEP YOUR PERSONAL DATA?

This section explains the length of time that we will retain your personal data. It also explains why we would hold your personal data for such time periods.

WHAT ARE YOUR RIGHTS?

This section explains that you have rights in relation to your personal data. It also explains what these rights are and how you can go about exercising them.

WHO CAN YOU ASK FOR MORE INFORMATION?

This section provides you with contact information should you have any questions or concerns about the way we handle your personal data. It also explains how you can contact the data protection regulator should you be unsatisfied with our response to your data protection issues.

1 ABOUT THIS PRIVACY NOTICE

1.1 We are committed to protecting the privacy and security of your personal data. Personal data is information that relates to an identified or identifiable individual. In this Privacy Notice we:

- set out how we use and protect the personal data that you provide to us;
- explain what we do with your personal data;
- explain your rights in relation to the personal data we hold about you; and
- tell you how you can contact us if you have any questions or comments.

1.2 **Principles:**

- compliance with this Privacy Notice will be monitored by the FirstGroup DPO and Deputy DPO (please see section 7 below) and reported on at a senior level to the FirstGroup plc Executive Committee.
 - any breach or attempted breach of this Privacy Notice will be viewed very seriously and we will take appropriate disciplinary action against any employee found to be facilitating a breach of this Privacy Notice. If any employee knows of, or suspects, that this Privacy Notice is not being complied with, you must tell your local Data Compliance Office, or the FirstGroup DPO or Deputy DPO (please see section 7 below), as soon as possible. Any report made in accordance with the guidelines set out in the Whistleblowing Policy will be treated confidentially.
- 1.3 This Privacy Notice may change from time to time and, if it does, the up-to-date version will always be available on the employee portal or on request from your HR representative. We will also tell you about any important changes to our Privacy Notice.

2 HOW WILL WE USE YOUR PERSONAL DATA?

2.1 We will collect, store and use information about you in order to carry out our activities and obligations as your employer. We will normally only do this where:

- it is necessary in order to comply with legal obligations which apply to us;
- it is necessary for the performance of your employment contract (including for the provision of any employee benefits that you elect or are awarded as part of your employment with us);
- it is necessary in order to fulfil our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests; or
- the law otherwise permits or requires it.

2.2 We may also use your personal information in the following situations, which are likely to be rare:

- where we need to protect your interests (or someone else's interests).
- where it is needed in the public interest.

2.3 Should you join or be awarded shares under any of the FirstGroup Share Plans then we may use any information you provide to us to administer your participation in any of the FirstGroup Share Plans.

2.4 In addition to the information that you provide to us, we may also collect, store and use information using the following means:

- CCTV, or other video and audio capture technology (for example, but not limited to, body-worn cameras) which we may use for the purposes of ensuring safety and for the prevention and detection of crime. Where we collect information through our use of CCTV we will only do so in compliance with our CCTV Policy which is available on the employee portal or on request from your HR representative.
- Audio recordings of telephone calls made or received on FirstGroup systems where recording functionality is enabled.
- Monitoring of your use of our IT systems, which includes our telephone systems. We will only ever monitor your use of our IT in compliance with our IT Acceptable Use Policy (UK and Ireland) which is available on the employee portal or on request from your HR representative.
- Access control systems and ANPR technology deployed at FGUK locations.
- Telematics software and platforms to locate and monitor driver/employee behaviour, measure performance and for safety purposes.

- Where our employees are required by law, or otherwise, to undergo any medical assessments or other regulatory checks (e.g. DVLA, DBS) to assure their ability to continue to fulfil the role in which they are employed.

We provide more details about the type of information we may collect and what it may be used for in Schedule 1. "Special categories" are particularly sensitive personal information and personal information relating to criminal convictions that require higher levels of protection. This includes information about your health, sex life, religious or philosophical beliefs, racial or ethnic origin and trade union membership. When we process special category personal data, we need to have further justification for collecting, storing and using this type of personal information. We have in place an appropriate policy document and safeguards which we are required by law to maintain when processing such data.

We may process special categories of personal information in the following circumstances:

- (a) In limited circumstances, with your explicit written consent.
- (b) Where we need to carry out our legal obligations or exercise rights in connection with employment.
- (c) Where it is needed in the public interest, such as for equal opportunities monitoring or in relation to our occupational pension scheme.

2.5 Less commonly, we may process this type of information where it is needed:

- (a) in relation to legal claims; or
- (b) to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

2.6 Where the personal information relates to criminal convictions and offences or related security measures we will only process this information where we have a legal right to do so. In most cases (although not necessarily all cases) this will be because the processing is necessary:

- (a) to comply with obligations we owe as a result of your employment or social security, or
- (b) for the purpose of assessing your working capacity.

2.7 We will use your particularly sensitive personal information in the following ways:

- (a) We will use information relating to leaves of absence, which may include sickness absence or family related leaves, to comply with employment and other laws.
- (b) We will use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits.
- (c) We will use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.
- (d) We will use trade union membership information to pay trade union premiums, register the status of a protected employee and to comply with employment law obligations.
- (e) We will use information relating to criminal convictions to assess your capacity to work.

2.8 We do not need your consent if we use special categories of your personal information in accordance with our written policy to carry out our legal obligations or exercise specific

rights in the field of employment law. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

2.9 Automated Decision Making

Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention. We do not envisage that any decisions will be taken about you using automated means, however we will notify you in writing if this position changes. You have rights in relation to automated decision making which are explained further in section 6 below.

3 WHO WILL HAVE ACCESS TO YOUR PERSONAL DATA?

3.1 Your personal data will only be seen or used by those of our employees who have a legitimate business need to access your personal data for the purposes set out in this Privacy Notice. This will include our HR team, your line management and other employees who need the information, or need access to the information, to perform their management or administrative functions.

3.2 We take your privacy seriously and have implemented appropriate physical, technical and organisational security measures designed to secure your personal data against accidental loss, destruction or damage and unauthorised access, use, alteration or disclosure.

4 WHO ELSE MIGHT WE SHARE YOUR PERSONAL DATA WITH?

4.1 Except as explained in this Privacy Notice, we will not share your personal data with third parties without your consent unless required to do so by law.

4.2 To comply with our legal, statutory and regulatory obligations we may share your personal data with HMRC and authorities including but not limited to the: Disclosure and Barring Service, Office of Rail and Road, Department for Transport, Rail Accident Investigation Branch, British Transport Police, Network Rail, Traffic Commissioner, Transport for London, Driver and Vehicle Standards Agency, Driver and Vehicle Licensing Agency, Rail Delivery Group, Rail Staff Travel Ltd, Railway Pension and Rail Assessment Centre Forum as appropriate from time to time.

4.3 We may share your personal data with third-party service providers who assist us with administering our employment relationship with you. This may include payroll processors, IT services providers, occupational health providers, workplace uniform providers, benefits administration providers, share plan administrators, trustees, insurance providers and legal services providers. Any such third parties will only be permitted to use your personal data for specific purposes in accordance with our instructions and not for their own purposes.

4.4 We may share your personal data with third parties to whom you are seconded to as part of your employment. This will include limited and basic personal information such as personal contact details (name, address, etc.), emergency contact information, government identification numbers. Any such third parties will only be permitted to use your personal data for specific purposes in accordance with our instructions and not for their own purposes.

4.5 We may share your personal data with third party professional service providers who assist us with establishing, exercising or defending legal rights. This may include insurance assessors and legal service providers. Any such third parties will only be permitted to use your personal data to the extent that we have appropriate obligations of confidentiality to ensure the protection of your personal data.

4.6 For reporting and administrative purposes, it may sometimes be necessary to share some of your personal data with other members of our group of companies.

- 4.7 If a business transfer or change of business ownership takes place or is envisaged, we may transfer your personal data to your new employer or a prospective new employer. If this happens, we will inform you of this transfer.
- 4.8 You acknowledge that the personal data that we collect from you may be transferred to, and stored at, a destination outside the UK or the European Economic Area (EEA) (as applicable, with consideration to the UK's exit from the European Union) and in countries not recognised by the European Commission or the relevant UK supervisory authority (as appropriate) as providing an adequate level of protection for personal data.
- 4.9 If we do transfer your personal data outside the EEA or the UK (as applicable), pursuant to paragraph 4.8 above, we will ensure that such transfer shall be covered by a framework recognised by the relevant authorities or courts as providing an adequate level of protection for personal data including, but not limited to, putting in place Standard Contractual Clauses (**SCCs**), as are in force from time-to-time.

5 HOW LONG DO WE KEEP YOUR PERSONAL DATA?

- 5.1 We will not retain personal data about you for any longer than is necessary. What is necessary will depend on the personal data in question and what it is needed for, including for the fulfilment of, any legal, accounting or reporting requirements imposed by law or regulation.
- 5.2 After your employment with us has ended, we will keep personal data about you in accordance with our Data Retention Policy, which is available on the employee portal or on request from your HR representative.
- (a) Personal data including your name, date of birth, National Insurance number and reason for leaving will be retained on a "leavers list". This information is kept to enable us to make informed recruitment decisions should you re-apply for employment with us (or any of our subsidiaries or associated entities) in the future.
- (b) If during your employment you join or are awarded shares under any of the FirstGroup plc Share Plans then the plan administrators will retain your information for so long as you remain a participant of any of the FirstGroup plc Share Plans and only to the extent that such information is relevant to the administration of the FirstGroup Share Plans.
- 5.3 We may retain personal data about you for statistical purposes (such as monitoring equality and diversity in our workplace). However, wherever possible, where data is retained for statistical purposes it will be anonymised.
- 5.4 For more information on our approach to retention, please see our Data Retention Policy, which is available on the employee portal or on request from your HR representative.

6 WHAT ARE YOUR RIGHTS?

- 6.1 It is important that the information we hold about you is accurate and up to date. If you think any of the personal data we hold about you is inaccurate or incomplete, you should let us know as soon as possible.
- 6.2 We hope that this Privacy Notice together with the policies we refer to in this Privacy Notice will provide you with the information you need about what personal data we are processing about you, why it is being processed, what we are using it for and how long it will be retained for. However, you have the right to access the personal data we hold about you by making a subject access request.
- 6.3 In some circumstances (e.g. if you think we are unnecessarily processing personal data about you), you may be able to ask us to erase your personal data, or to stop or restrict the processing your personal data. You may also request that we transfer your personal data to another party.

- 6.4 You have the right to object to automated decision-making. This is where a decision, which produces legal effects or similarly significantly affects you, has been based solely on automated processing (including profiling). We are allowed to use automated decision making in the following circumstances:
- (a) Where we have notified you of the decision and given you 21 days to request a reconsideration.
 - (b) Where it is necessary to perform the contract with you and appropriate measures are in place to safeguard your rights.
 - (c) In limited circumstances, with your explicit written consent and where appropriate measures are in place to safeguard your rights.
- 6.5 If we make an automated decision on the basis of any particularly sensitive personal information, we must have either your explicit written consent or it must be justified in the public interest, and we must also put in place appropriate measures to safeguard your rights.
- 6.6 For more information on your rights and how to use them, or if you would like to exercise any of your rights, please contact us using the details set out in section 7 below.

7 WHO CAN YOU ASK FOR MORE INFORMATION?

- 7.1 FirstGroup plc (and its relevant subsidiaries or associated entities) are data controllers, because we collect personal data about you and determine how and why it will be used. Our contact details are: post: FAO Data Protection Officer, 8th Floor, The Point, 37 North Wharf Road, London W2 1AF; tel: +44 (0)20 7291 0505; or email: DPO@firstgroup.co.uk
- 7.2 We have appointed Christy Baker as the FirstGroup Data Protection Officer and Beth Sharratt as the Deputy Data Protection Officer. They are responsible for our approach to data protection and protecting your privacy. You can contact them at DPO@firstgroup.co.uk
- 7.3 Within each FirstGroup company we also have a Data Compliance Officer and, in some cases, Data Protection Champions. You can find the details of your organisation's Data Protection Champions on the employee portal. You may also ask them any queries you have in relation to this Privacy Notice and the use of your personal data.
- 7.4 If you are unsatisfied with our response to any data protection issues you raise with us or the Data Protection Officers, you have the right to make a complaint to the Information Commissioner's Office (ICO). The ICO is the authority in the UK which is tasked with the protection of personal data and privacy. Alternatively, if you are a resident of, or work in, the Republic of Ireland, you have the right to make a complaint to the Irish Data Protection Commission.

Schedule 1

TYPE OF PERSONAL DATA	WHAT IT MAY BE USED FOR
Personal contact details such as name, title, address, telephone numbers and email address	To contact you, for business management and planning and for the administration of benefits and share plans
Date of birth	For equal opportunity monitoring and reporting, to ensure compliance with our legal obligations, for business management and planning and for the administration of benefits and share plans
Gender	For equal opportunity monitoring and reporting, and to ensure compliance with our legal obligations e.g. gender pay reporting
Details of partner and dependants such as names, date of birth, gender	To administer benefits to which your family may also be entitled such as travel passes, life insurance and medical cover
Emergency contact information	To contact your next of kin in the event of an emergency
Government identification numbers (e.g. social security, national insurance, driver's licence, passport)	To verify your identity, to administer payroll and benefits accurately, to comply with our legal obligations and for the administration of benefits and share plans
Bank account details and payroll information	To pay you (including reimbursement of expenses) and for the proceeds of any share sales to be remitted to you
Wage and benefit information (including pensions information)	To monitor and administer your salary, benefits and share awards (if applicable) and for business management and planning. To comply with our legal obligation on gender pay reporting
Performance information	To monitor, assess and improve workplace performance, to identify training needs, for business management and succession planning and, if necessary, investigate allegations of misconduct
Start date	To ensure your employment rights are honoured, to ensure you receive the correct benefits, for business management and planning and to monitor your length of service.
Education and training records	To ensure you have and maintain the correct qualifications and skills to perform your role and identify any future training needs

Professional membership records	To ensure you have the relevant memberships required or desirable in order to perform your role
References, assessment records, CVs, cover letters and work history	To validate your qualifications and evidence your suitability for your role
Proof of work eligibility e.g. passport, birth certificate, biometric residence permit	To provide evidence that you have the right to work or to sponsor you to obtain such a right
Criminal records checks	To ensure and evidence your suitability for your role
Photograph	To verify your identity and for internal communications
IT records (through use of our IT equipment) which includes internet usage and content of emails	To ensure network and information security and, if necessary, to detect and prevent fraud or inappropriate usage and, if necessary, investigate allegations of misconduct
Telephone records	To ensure network and information security, to detect and prevent fraud or inappropriate usage and, if necessary, investigate allegations of misconduct
Race, nationality or ethnic origin and religious or philosophical beliefs	For equal opportunity monitoring and reporting, and to ensure compliance with our legal obligations
Sexual orientation	For equal opportunity monitoring and reporting, and to ensure compliance with our legal obligations
Health records	To ensure public safety and employee safety in the workplace and to provide appropriate adjustments to enable you to remain in or return to work
Attendance records, including details relating to Maternity, Paternity, Shared Parental and Adoption leave and pay	To monitor attendance levels, to ensure employee safety in the workplace, to provide appropriate workplace adjustments (e.g. to ensure correct payment of work time, overtime, annual leave, etc.) and for business management and planning
Conduct information (including disciplinary and grievance records)	To monitor and, if necessary, address your conduct
Trade union membership	For trade union administration and to ensure compliance with our legal obligations
CCTV and body-worn camera footage	To ensure building security of FirstGroup assets and safety of employees, customers and members of the public (which may include the investigation of any reported incidents that take place)

Voice recordings	To retain verbal evidence in relation to any safety or operational incidents
Travel arrangements and working location	To enable us to account for your presence, and to contact you in the event of an emergency
Records of expenses incurred on your corporate credit card, or reimbursed to you through payroll	To monitor corporate expenditure and to ensure compliance with expenses policy
Location data (e.g. records of entry and exit to the building or car park and, in case of emergency, fire evacuation)	To ensure building security, in case of emergency, to ensure that all parties within the building have been safely evacuated and, if necessary, to investigate allegations of misconduct
Personal measurements	To provide you with the uniform/ protective clothing required to carry out your role
Talent management and succession planning data	To identify talent to support employee development and succession planning
IP address	To ensure network and information security and, if necessary, to detect and prevent fraud or inappropriate usage

Please note that, in the event of a dispute between us and you, any of the information set out above may be used to establish and defend a legal claim.

HOW WE USE YOUR PERSONAL DATA: KEY THINGS YOU NEED TO KNOW

As your employer, we need to use your **personal data**. We need to do this for a number of reasons including where: we are required by **law** to process your personal data, it is **necessary** for the performance of your **employment contract**, where we have **legitimate interests** in processing your personal data (and only where your interests and rights do not override our interests) or the **law** otherwise permits it.

Please note: generally, we do not need your consent to process your personal data. Only in very limited circumstances will we ask for your consent. If we do ask for consent you are under no obligation to provide it and if you decide not to, it will not affect your contract of employment with us.

What personal data do you collect about me?

We collect data such as your name, date of birth or home address. We also collect more sensitive information, referred to as "special category" personal data, which concerns things such as your health.

As well as the data you give to us, we may also collect, store and use information using things such as CCTV or body-worn videos, audio recordings or monitoring your use of our IT systems. We will only ever do this in accordance with the relevant policies we have in place.

A full list of the personal data we collect, store and use can be found in Schedule 1 of our Employee Privacy Notice.

How do you use my data?

We collect, store and use your personal data to carry out our activities and obligations as your employer.

There are a number of reasons we might use your data. For example, to pay you and to administer your employment benefits. There are other reasons too, such as where we need to establish, exercise or defend legal rights (for example, if a legal claim is made against our business).

We will always use your personal data in compliance with the applicable laws and this Privacy Notice.

Details of how we use your data are in Section 2 of our Employee Privacy Notice, which is available on the employee portal.

Where can I get more information?

We are committed to protecting the privacy and security of your personal data.

If you would like more information about how we process your personal information, please read our Employee Privacy Notice.

If you have any questions, you can also ask:

- your Data Compliance Officer or, if you have one, your Data Protection Champion – all details are on the employee portal
- if they are unable to help, you can contact the Deputy Data Protection Officer by emailing DPO@firstgroup.co.uk

If you become aware of or suspect a breach of our Employee Privacy Notice, you **must** tell us. Details about how to do this are in Section 1.2 of the Employee Privacy Notice.