Data Protection Policy Statement

Why it matters

Our values and ethical commitment shape not only what we do, but also how we do it. We invest time and effort to put in place the right processes, policies and governance structures to ensure we meet these high standards of integrity and professionalism.

At FirstGroup plc, and across our operating companies, we respect and protect everyone's privacy, and comply with all applicable data protection laws. In summary, this means we:

(i) process personal data in a manner that is appropriate and lawful;

(ii) take appropriate steps to protect the confidentiality, integrity and accessibility of personal data; and

(iii) ensure individuals are able to exercise their privacy rights.

Why is personal data important?

To run our business effectively and efficiently, we need to collect and use personal data relating to our employees, customers, suppliers and third parties. Processing personal data enables us to manage our employees, provide the best possible offering to our customers and help to keep everyone in our communities safe.

We are committed to complying with all applicable data protection laws including:

- UK General Data Protection Regulation;
- Data Protection Act 2018; and
- EU General Data Protection Regulation.

We acknowledge that a breach of our legal obligations may have serious consequences on the individual(s) involved, as well as potentially impacting the reputation of FirstGroup plc and our operating companies.

Our expectations

All employees commit to complying with the law and our policies. For data protection, relevant employees must make an annual declaration that they have read and understood our FirstGroup Data Protection Policy, and ensure they complete mandatory data protection training each year.

Our FirstGroup Data Protection Policy sets out a minimum standard and provides clear guidance to our employees on how personal data must be treated in order to comply with our obligations under the law. It also explains key concepts of the legislation and provides employees with points of escalation when further advice or action is required.

Employees must also comply with the FirstGroup Acceptable Use Policy which sets out the rules on appropriate and safe use of FirstGroup systems and/or devices.

We have a Data Protection Officer and Deputy Data Protection Officer in place who are appropriately skilled, operate with independence and are granted all necessary authority in the performance of their tasks. There is an established network of Data Compliance Officers embedded across our business who are responsible for day-to-day compliance.

Our expectations continued

Privacy notices are published to ensure that FirstGroup satisfies its obligation to provide certain information to individuals when personal data is collected. Each FirstGroup business is required to have a public-facing privacy notice and an employee privacy notice.

Our Supplier Code of Conduct requires any supplier, service provider or other third party that processes personal data on our behalf to enter into a contract which includes appropriate data protection provisions. Where appropriate, and prior to entering into a contract, due diligence is conducted.

Our Information Security team ensure we have appropriate technical controls in place to safeguard the integrity and confidentiality of the personal data we process. They are responsible for monitoring and assessing threats and responding to attempted attacks on our systems. We have procedures in place to manage data security incidents appropriately, including making appropriate notifications to regulators and other stakeholders, as well as informing the affected individual(s) where required. We regularly conduct data security breach exercises across our businesses and develop our incident response based on lessons learnt from those exercises, as well as from live incidents and from incidents experienced by other organisations.

Compliance

All colleagues must comply with the relevant policies and any failure to do so will be treated seriously and may result in disciplinary action.

We monitor compliance using a range of measures including:

- Group Internal Audit engagements
- Complaints received from individuals
- Correspondence from regulators
- Training completion statistics
- DPIA reviews
- Queries received from the businesses

Speak up

If you have any concerns, you should raise it with your line manager in the first instance, who should be able to address it quickly and effectively or escalate it on your behalf where necessary. If the concern involves your line manager, you'd prefer not to raise it with them, or they have previously not addressed the issue, you can either raise it with their line manager or with your HR team. Alternatively, you can contact our independently run Confidential Reporting Hotline either by telephone or online.

The Confidential Reporting Hotline numbers are:

- UK **0808 234 5291**
- IRELAND **1-800 552 083**

You can also use the Web Portal at **www.firstethics.ethicspoint.com.**

We support honest and open communication and encourage everyone to ask questions and report concerns. We do not tolerate retaliation, and consider it to be serious misconduct.

Policy Owner	FirstGroup Data Protection Officer
Compliance Lead	FirstGroup Data Protection Officer
Published	October 2023
Frequency of review	Annual
Next review date	October 2024