



Privacy Policy



If you need this publication in larger print, audio, Braille, or in another language, please get in touch and we will be happy to help.

Date Approved: August 2026

Next Reviewed: August 2031

1. Introduction

The Kingdom Group (Kingdom) is committed to ensuring the secure and safe management of all data relating to our customers, staff and other individuals. Our staff members have a responsibility to ensure compliance with the terms of this policy, and to manage individuals' data in accordance with this policy.

Kingdom needs to gather and use certain information about individuals in order to provide a service. This means that Kingdom manages a significant amount of data, from a variety of sources across the Group structure. This data contains Personal Data and Sensitive Personal Data (known as Special Categories of Personal Data under the UK GDPR).

This policy sets out our duties in processing that data, and the purpose of this policy is to set out the procedures for the management of such data.

The Data (Use and Access) Act 2025 ("DUA") and associated regulations will make changes to data protection law, meaning that the functions of the Information Commissioner will be transferred to the Information Commission. At the time of preparing this policy, these changes are yet to come into force. Until these changes come into force, references in this policy to the "Information Commission" should be treated as a reference to the Information Commissioner.

2. Legislation

It is a legal requirement that Kingdom must collect, handle and store personal information in accordance with the relevant legislation.

The relevant legislation in relation to the processing of data is:

- The UK General Data Protection Regulation (the "GDPR")
- The Privacy and Electronic Communications (EC Directive) Regulations 2003
- The Data Protection Act 2018 ("the 2018 Act") and
- Any legislation that, in respect of the United Kingdom, replaces or enacts into United Kingdom domestic law, the UK GDPR, the Privacy and Electronic Communications (EC Directive) Regulations 2003 or any other law relating to data protection, the processing of personal data

and privacy as a consequence of the United Kingdom leaving the European Union.

3. Data

Kingdom holds a variety of Data relating to living individuals, including customers and employees (also referred to as data subjects). Data which can identify Data Subjects and related to them is known as Personal Data. The Personal Data held and processed by us is detailed within the Fair Processing Notice.

“Personal Data” is that from which a living individual can be identified either by that data alone or in conjunction with other data held by Kingdom and which relates to that individual.

Kingdom also holds Personal data that is sensitive in nature (i.e. relates to or reveals a data subject’s racial or ethnic origin, religious beliefs, political opinions, relates to health or sexual orientation). This is known as “Special Category Personal Data” or “Sensitive Personal Data”. The Secretary of State may designate further categories of Special Category Personal Data, and if this occurs, we shall treat any such designated data accordingly.

4. Processing of Personal Data

Kingdom is permitted to process Personal Data on behalf of data subjects, provided it is doing so on one of the following grounds:

- Processing with the consent of the data subject;
- Processing is necessary for the performance of a contract between Kingdom and the data subject or for entering into a contract with the data subject;
- Processing is necessary for Kingdom’s compliance with a legal obligation.
- Processing is necessary to protect the vital interests of the data subject or another person;
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of Kingdom’s official authority; or
- Processing is necessary for the purposes of legitimate interests pursued by Kingdom or by a third party; or
- Processing is necessary for the purposes of a recognised legitimate interest

Fair Processing Notice

Kingdom has produced a Fair Processing Notice (FPN) which it is required to provide to all customers whose Personal data is held.

The Fair Processing Notice sets out the Personal Data processed by Kingdom and the basis for that Processing.

This document is provided to all of Kingdom's customers at the outset of processing their data.

Employees

Details of the data held and processing of that data is contained within the Employee Fair Processing Notice. A copy of any employee's Personal Data held by us is available upon written request by that employee to their Line Manager, HR Officer or Data Protection Officer.

Board Members

Details of the data held and proceeding of that data is contained within the Board Member Fair Processing Notice. A copy of any Board Members Personal Data held by us is available upon request by that Board Member to the Governance team.

Consent

Consent as a ground of processing personal data will only be used by us where no other alternative ground for processing is available. If Kingdom requires to obtain consent to process a Data Subject's Personal Data, it shall obtain that consent in writing unless extenuating circumstances apply. The consent provided by the Data Subject must be freely given, and the Data Subject will be required to sign a relevant consent form if willing to consent. Any consent to be obtained by Kingdom must be for a specific and defined purpose. Where consent is being relied on, Data Subjects are free to withhold their consent or withdraw it at any future time.

Processing of Special Category Personal Data or Sensitive Personal Data

In the event that we process Special Category Personal Data or Sensitive Personal Data, we will do so in accordance with one of the following grounds of processing:

- The data subject has given explicit consent to the processing of this data for a specified purpose;

- Processing is necessary for carrying out obligations or exercising rights related to employment or social security, or social protection law;
- Processing is necessary for health or social care;
- Processing is necessary to protect the vital interests of the data subject or, if the data subject is incapable of giving consent, the vital interests of another person;
- Processing is necessary for the establishment, exercise or defence of legal claims, or whenever courts are acting in their judicial capacity; and
- Processing is necessary for reasons of substantial public interest under law

5. Data Sharing

Kingdom shares its data with various third parties for numerous reasons in order that its day to day activities are carried out in accordance with our relevant policies and procedures (e.g. for processing of the employees' pension). Both Kingdom and the third party will be processing that data in their individual capacities as data controllers. To monitor compliance by these third parties with Data Protection laws, we require the third party organisations to enter into a Data Sharing Agreement with us, governing the processing of data, security measures to be implemented and responsibility for breaches.

Data Processors

A data processor is a third party entity that processes personal data on behalf of us, and are frequently engaged if certain types of Kingdom's work is outsourced (e.g. gas servicing works). A data processor must comply with the same Data Protection laws as Kingdom.

A processor must comply with Data Protection laws. Kingdom's processors must ensure they have appropriate technical security measures in place, maintain records of processing activities and notify Kingdom if a data breach is suffered.

If a processor wishes to sub-contract their processing, prior written consent of Kingdom must be obtained. Upon a sub-contracting of processing, the processor will be liable in full for the data protection breaches of their sub-contractors.

Where we contract with a third party to process personal data held by us, we require the third party to enter into a contract (a Data Protection Addendum).

6. Data Storage and Security

All Personal Data held by us will be stored securely, whether electronically or in copy format.

Paper Storage

If personal data is stored on paper, it should be kept in a secure place where unauthorised personnel cannot access it. Employees should ensure that no Personal Data is left in a place where unauthorised personnel can access it. When the personal data is no longer required (following Kingdom's retention policy), it must be disposed of by the employee so as to ensure its secure destruction. If the Personal Data requires to be retained on a physical file, then the employee should ensure that it is affixed to the file, which is then stored in accordance with Kingdom's storage provisions.

Electronic Storage

Personal Data stored electronically must also be protected from unauthorised use and access. Personal Data must be protected by appropriate security controls when being transferred internally or externally to Kingdom's processors or to organisations with whom Kingdom has entered into a Data Sharing Agreement.

If Personal Data is stored on removable media (CD, DVD, USB memory stick), then it must always be encrypted and stored securely. Personal Data should not be saved directly to mobile devices and should be stored on designated drives and servers.

7. Breaches

A data breach can occur at any point when handling Personal Data and we have reporting duties in the event of a data breach or potential breach occurring. Breaches which pose a risk to the rights and freedoms of the data subjects who are subject of the breach require to be reported externally to the Information Commissioner's Office (ICO) within 72 hours of the breach occurring.

Kingdom takes the security data very seriously and, in the unlikely event of a breach, will take the following steps:

- As soon as it becomes known that a breach or potential breach has occurred, our DPO must be notified in writing of the breach, how it occurred and what the likely impact of that breach is on any data subject(s);
- Kingdom must seek to contain the breach by whichever means available;
- The DPO must consider the breach is one which requires to be reported to the IC and to the Data Subjects affected;
- Notify third parties in accordance with the terms of any applicable Data Sharing Agreements, Data Processing Agreements or equivalent contract terms.

8. Data Protection Officer (DPO)

A Data Protection Officer is an individual who has an overarching responsibility and oversight over compliance with Data Protection laws. Kingdom has elected to appoint Calum Kippen, Director of Governance, and Communications as the Data Protection Officer. His details are noted on our website and contained within the Fair Processing Notice. The DPO will be responsible for:

- Monitoring compliance with Data Protection laws and this policy and advising on compliance needed;
- Co-operating with and serving as the contact for discussions with the IC;
- Reporting breaches or suspected breaches to the IC and data subjects

9. Data Subject Rights

Certain rights are provided to data subjects under the GDPR. Data Subjects are entitled to view the personal data held about them by us, whether in written or electronic form.

- a right to be informed about the collection and use of their personal data (typically fulfilled by providing individuals with a Fair Processing Notice) (the “right to be informed”);
- a right to access and receive a copy of their personal data, plus other supplementary information (the “right of access”);
- a right to have inaccurate personal data rectified and incomplete personal data completed (the “right to rectification”);
- a right to have personal data erased (the “right to erasure”);

- the right to request the restriction or suppression of personal data (the “right to restrict”);
- the right to obtain and reuse certain personal data across different providers (the “right to data portability”);
- the right, in certain circumstances, to object to the processing of their personal data (the “right to object”);
- the right to make a complaint about how their personal data has been processed (the “right to complain”); and
- rights to protect individuals against automated decision making or profiling (“rights related to automated decision making”).

These rights are notified to the Association’s tenants and other customers in the Association’s Fair Processing Notice. Such rights are subject to qualification and are not absolute.

Subject Access Requests

Data Subjects are permitted to view their personal data held by us upon making a request to do so (a Subject Access Request). Upon receipt of a request by a data subject, we will respond to the Subject Access Request within one month of the date of receipt of the request. Kingdom:

- must provide the data subject with an electronic or hard copy of the personal data requested, unless any exemption to the provision of that data applies in law.
- where the Personal Data comprises data relating to other Data Subjects, the Association shall only release that data where: the Association has obtained consent from those Data Subjects OR the Association determines it is reasonable to disclose said data without consent. or
- where the Association does not hold the Personal Data sought by the Data Subject, must confirm that it does not hold any or that Personal Data sought to the Data Subject as soon as practicably possible, and in any event, not later than one month from the day after the date on which the request was made.

The Right to Erasure

A data subject can exercise their right to erasure by submitting a request in writing to the DPO seeking that we erase the data subject’s Personal Data in its entirety.

Each request received by our DPO will require to be considered on its own merits and legal advice will require to be obtained in relation to such requests from time to time. The DPO will have responsibility for accepting or refusing the data subject's request and will respond in writing to the request. Requests for Erasure will be considered and responded to by the DPO by one month from the day after the date we receive the request unless Kingdom is entitled to increase the timescales under relevant legislation.

The Right to Restrict or Object to Processing

A data subject may request that we restrict our processing of the data subject's Personal Data, or object to the processing of that data.

In the event that any direct marketing is undertaken from time to time by us, a data subject has an absolute right to object to processing of this nature, and if we receive a written request to cease processing for this purpose, then we will do so.

Each request received by us will require to be considered on its own merits and legal advice will require to be obtained in relation to such requests from time to time. The DPO will have responsibility for accepting or refusing the data subject's request and will respond in writing to the request.

The Right to Rectification

A Data Subject may request to have inaccurate Personal Data rectified.

If appropriate, a Data Subject may also request to have incomplete Personal Data completed.

Each request received by Kingdom will require to be considered on its own merits and legal advice will require to be obtained in relation to such requests from time to time. The DPO will have responsibility for accepting or refusing the Data Subject's request and will respond in writing to the request.

The Right to Data Portability

A Data Subject may ask for their personal data which they have provided to Kingdom to be provided in a structured, commonly used, machine readable format or the Data Subject may ask for this data to be transmitted directly to another organisation. This is subject to certain exemptions.

Each request received by Kingdom will require to be considered on its own merits and legal advice will require to be obtained in relation to such

requests from time to time. The DPO will have responsibility for accepting or refusing the Data Subject's and will respond in writing to the request.

The Right to Complain

A Data Subject may complain to Kingdom if they consider their personal data has been processed by us in contravention of Data Protection Law. Any such complaint shall be handled in accordance with Kingdom's Compliments and Complaints Policy.

Rights Related to Automated Decision Making

Should Kingdom utilise any automated decision making it shall follow the requirements set down in data protection law to protect the Data Subjects in question.

10. Privacy Impact Assessments (PIAs)

These are a means of assisting us in identifying and reducing the risks that our operations have on personal privacy of data subjects. Whilst this policy uses the term PIAs, it is also recognised that these assessments are also commonly referred to as "Data Protection Impact Assessments" or similar. Kingdom shall:

- carry out a PIA before undertaking a project or processing activity which poses a "high risk" to an individual's privacy e.g. the implementation of a new computer system or software which involves processing personal data; and
- in carrying out a PIA, include a description of the processing activity, its purpose, an assessment of the need for the processing, a summary of the risks, and details of any security measures that need to be taken to protect the personal data

Kingdom will be required to consult the IC in the event that a PIA identifies a high level of risk which cannot be reduced or mitigated. The DPO will be responsible for such reporting, and where a high level of risk is identified by those carrying out the PIA, they are required to notify the DPO within five (5) working days.

10. Archiving, Retention and Destruction of Data

We will not retain Personal Data indefinitely; we will ensure that Personal Data is only retained for the period necessary. We shall ensure that all personal data is archived and destroyed in accordance with our Data Retention Guidelines, which are regularly reviewed

Document Control

Prepared by	Governance & Communications
Was AI used in preparing this policy?	No
References used	UK General Data Protection Regulation (UK GDPR) Data Protection Act 2018 (DPA 2018) Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) Data (Use and Access) Act 2025 (and associated amendments to UK data protection law) SFHA Model Policy
Circulation	Data Protection and Freedom of Information Working Group
Approved by	Audit, Finance & Risk Committee
Review frequency	Every 5 years unless an earlier review is required
Next review date	August 2031