

DATA PROTECTION POLICY

Responsible Officer	Head of Governance
Effective Date	26/11/2024
Next Review Date	26/11/2026
Associated Documents	Employee's Contract of Employment, Employment Terms and Conditions, Confidentiality Policy, Responsible AI Policy, Data Subject Request Policy and Response Procedure, Privacy Notice
Document version	V.3

© Retail Trust | retailtrust.org.uk
Retail Trust is a registered charity in England and Wales (1090136) and in Scotland (SC039684). Company No 4254201 (Company limited by Guarantee) Registered England & Wales. Registered office: Retail Trust, The Form Rooms, Second Floor, 22 Tower Street, London, WC2H 9NS

1. Introduction.

At Retail Trust, we understand the importance of safeguarding the personal data we handle. We collect, store, and process personal information about trustees, employees, residents, contractors, consultants, volunteers, and other third parties.

We are committed to managing this data responsibly and in full compliance with applicable laws. Our approach is based on the principles set out in Data Protection Legislation, ensuring that all personal data is processed fairly, lawfully, and transpa rently. This policy outlines Retail Trust's guidelines for data protection and the legal requirements that must be met regarding the colle ction, handling, processing, storage, transportation, and disposal of personal information.

The purpose of this policy is to provide clear guidelines for managing personal data in a way that ensures compliance with the Data Protection Act 2018 (DPA) and the General Data Protection Regulation (GDPR) (EU) 2016/679, as incorporated into UK law following the European Union (Withdrawal) Act 2018. This policy applies to all employees, trustees, volunteers, contractors, consultants, residents, and third parties acting on behalf of Retail Trust.

2. Scope

This policy applies to all employees of Retail Trust, as well as trustees, residents, contractors, consultants, volunteers, a nd other third parties acting on behalf of Retail Trust, who are based in the United Kingdom or process the personal data of indivi duals residing in the United Kingdom. This policy does not form part of any employee's contract of employment and may be revised at any time.

Personal data, whether stored in paper form or electronically (e.g., on computers or other media), is subject to specific leg al safeguards outlined in the Data Protection Act 2018 (DPA) and other relevant laws or regulations. The Data Protection Act pla ces certain restrictions on how Retail Trust can use personal data.

3. Data Protection Principles

Retail Trust is committed to ensuring that all personal data is:

- processed lawfully, fairly and in a transparent manner.
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with these purposes.
- adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
- accurate and where necessary, kept up to date.
- not kept for longer than is necessary for the purpose it was collected.
- processed in a manner that ensures appropriate security of the personal data including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage.
- stored in a manner that ensures data subjects can be identified only if necessary for the purposes for which it was collected.
- use appropriate technical and organisational measures to protect personal data from unauthorised access, loss, or destruction.
- retained for no longer than is necessary for the purposes for which it was collected.

4. Legal Basis for Processing Personal Data

Retail Trust will only process personal data where there is a lawful basis for doing so. The lawful bases for processing incl ude:

- consent from the data subject
- performance of a contract with the data subject
- legal obligation
- legitimate interests pursued by Retail Trust or a third party
- protection of vital interests
- performance of a task carried out in the public interest or in the exercise of official authority.

5. Processing for limited purposes.

Personal data will only be processed for the specific purposes for which it was originally collected, as notified to the Data Subject at the time of collection, or for other purposes explicitly permitted by the Data Protection Act. This means that personal data will not be collected for one purpose and then used for a different, unrelated purpose.

If it becomes necessary to change the purpose for which personal data is processed, the Data Subject will be informed of the new purpose before any processing takes place. In such cases, the Data Protection Team must be contacted, and a Data Protection Impact Assessment (DPIA) must be conducted prior to processing personal data for any new purpose.

The specific purposes for which personal data will be processed are outlined in our Privacy Notice.

6. Processing special categories of personal data

Where information relates to an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership or involves genetic data, biometric data, data concerning health or an individual's sex life or sexual orientation, this is known as "special categories of personal data". Retail Trust may only process special categories of personal data where one of the conditions above applies **and** one of the following applies:

The individual has given their explicit consent for us to process their personal data;

- the personal data is required for us to comply with our obligations under employment, social security, or social protection law. For example, we are required to maintain employees' absence records as an employer;
- the personal data is necessary in order to protect the vital interests of the individual. This only applies for matters of life and death. For example, the disclosure of an individual's medical history to a hospital casualty department treating them;
- the processing relates to personal data that has manifestly been made public by the individual;
- the personal data is required to establish, exercise, or defend legal claims. For example, we need to refer to or rely on personal data in order to defend an action raised against us in court;
- the processing of the personal data is necessary for reasons of substantial public interest under law. For example:

(a) to prevent or detect unlawful acts by disclosing personal data to the police;
(b) to identify or keep under review the existence or absence of equality of opportunity or treatment between groups of people specified in relation to that category with a view to enabling such equality to be promoted or maintained;
(c) to provide support to individuals with a particular disability or medical condition or raise awareness of that disability or medical condition;
(d) to provide confidential counselling, advice, or support;
(e) to safeguard individuals and children at risk to protect an individual from neglect or physical, mental, or emotional harm, or the physical, mental, or emotional well-being of an individual; or
(f) to safeguard the economic wellbeing of certain individuals;

- the processing of the personal data is necessary for health or social care purposes. For example, to assess the working capacity of an employee or provide social care; or
- the processing is necessary for reasons of public interest in the area of public health were processed by a health professional or under a duty of confidentiality. For example, to protect against cross-border threats to health.

7. Data Subject Rights.

Data subjects (individuals whose data is being processed) have certain rights regarding their personal data. These include the right to:

- the right to request access to and a copy of their personal data.
- right to be informed/ provided with information on how their data will be handled, as outlined in the Privacy Notice.
- The right to rectify inaccurate or incomplete personal data.
- the right to request deletion/ erasure of personal data in certain circumstances, such as when it's no longer needed or unlawfully processed, subject to exemptions.

- the right to restrict processing in cases where the data is being processed unlawfully or while objections or complaints are resolved.
- the right to obtain and reuse personal data for their own purposes or transfer it to a third party, applicable to automated processing and consent-based data.
- the right to object to processing based on public interest, legitimate interests, or for direct marketing. In the case of direct marketing, the request must be actioned immediately.
- the right to avoid decisions based solely on automated processing, including profiling, that have legal effects or similarly significant consequences.

The foregoing right does not apply if:

(a) it is necessary to enter a contract with the data subject and Retail Trust;
(b) it is authorised by applicable law (and such law lays down suitable measures to safeguard the data subjects' rights and freedoms and legitimate interest) or (c) is based on the data subject's explicit consent.

However, even if (a) or (c) is relevant, please note that Retail Trust must put in place suitable measures to safeguard the rights of the data subject including the right to ask for a human to review the decision on behalf of Retail Trust and to contest the decision. Further, automated decision-taking based on special category of data can only be done with explicit consent.

Requests related to data subject rights should be directed to the Data Protection Officer (DPO) or designated staff member.

For Email Requests: immediately forward the request to the Head of Governance at dataprotection@retailtrust.org.uk and include "CONFIDENTIAL" in the subject line.

For Letter Requests:

- scan the letter and email an encrypted copy to the above address.
- post the original letter to the Head of Governance (address provided).

RetailTrust
Eborn house, Leylands Estate, Broadway,
Derby, DE22 1AY

All written requests must be dated stamped or signed on receipt.

Requests will be dealt with the Data Protection Officer; they will need to consult other members of staff who may be holding the personal data requested or in order to determine what information falls within the scope of the request.

The Data Protection Officer (DPO) is responsible for determining the validity of each request. If necessary, the DPO may contact the requestor to obtain additional information before processing the request. Retail Trust will respond to all requests within one month of verifying the requestor's identity and receiving all necessary information. In cases where requests are complex or numerous, the response time may be extended by up to two additional months. The DPO will inform the requestor of any such extension and the reasons for it.

Refusing a Data Subject request.

We would refuse to supply the information where:

- we are not satisfied that the requester is the individual concerned (or their appointed representative);
- the subject access rights under the Data Protection Legislation do not apply; or
- all the information requested is exempt.

In responding to the request, the Data Protection Officer will set out clearly the reasons for refusal, such as any specific exemptions that apply, and any additional information which is thought will help the requestor to understand the reason for refusal.

© Retail Trust | retailtrust.org.uk
Retail Trust is a registered charity in England and Wales (1090136) and in Scotland (SC039684). Company No 4254201 (Company limited by Guarantee) Registered England & Wales. Registered office: Retail Trust, The Form Rooms, Second Floor, 22 Tower Street, London, WC2H 9NS.

We would not refuse to deal with a request on the basis that some of the personal data is exempt. In such cases we should provide the personal data that is not exempt and clearly explain why other personal data requested cannot be supplied. Where we decide not to act in response to a request, we must explain why to the individual and let them know that they can complain to the **ICO** or seek a remedy through the courts.

8. Timescale for dealing with subject access requests

We must comply with a request promptly and in any event within one month of receipt of a valid request and submission of all verification details.

Where the request is such that it cannot be dealt with promptly because it is complex or voluminous, we should contact the Data Subject acknowledging their request and explaining reasons for the delay. We may be able to extend the time period for responding to any complex and numerous requests by two months. This time period is set out in the Data Protection Legislation and must be complied with.

10. Data Sharing and Third Parties

Retail Trust may share personal data with third parties where necessary, in accordance with the Data Protection Legislation. Any third party that receives personal data will be required to comply with strict data protection requirements to ensure the confidentiality and security of the data.

Personal data will not be transferred outside of the United Kingdom or the European Economic Area (EEA) unless appropriate safeguards are in place to protect the data.

11. Data Retention

Retail Trust will retain personal data for no longer than necessary to fulfil the purposes for which it was collected, or as required by law. Once personal data is no longer required, it will be securely destroyed or removed from our IT systems, as far as reasonably possible.

12. Breach Notification

In the event of a data breach, Retail Trust will take immediate steps to mitigate any harm caused by the breach and will notify the Information Commissioner's Office (ICO) by law within 72 hours of us becoming aware of the breach and affected individuals where required.

13. Responsibilities

Data Protection Officer (DPO): the DPO is responsible for overseeing Retail Trust's compliance with this policy and the Data Protection Legislation, providing advice on data protection matters, and managing data protection requests.

Employees and Contractors: all employees, contractors, and third parties with access to personal data must comply with this policy and ensure that personal data is processed securely and lawfully.

Managers and Trustees: managers and trustees must ensure that staff members are trained in data protection practices and that personal data is processed in compliance with this policy. **14. Policy Review**

This policy will be reviewed at regular intervals to ensure its effectiveness and continued compliance with data protection laws. Any amendments to this policy will be communicated to all staff and relevant stakeholders.

© Retail Trust | retailtrust.org.uk
Retail Trust is a registered charity in England and Wales (1090136) and in Scotland (SC039684). Company No 4254201 (Company limited by Guarantee) Registered England & Wales. Registered office: Retail Trust, The Form Rooms, Second Floor, 22 Tower Street, London, WC2H 9NS.