



CONFIDENTIALITY POLICY

Responsible Officer	Head of Governance & Head of HR
Effective Date	14/10/2024
Next Review Date	14/10/2026
Associated Documents	Employee's Contract of Employment, Data Protection Policy, Responsible AI Policy
Document version	v.2



© Retail Trust | Retail TRUST.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: Marshall Estate, Hammers Lane, London, NW7 4DQ.

1. Introduction.

Retail Trust recognises that during your involvement with the Trust, you will have access to confidential information. To ensure that everyone interacting with the Trust can do so with confidence, this policy outlines how we promote a culture of confidentiality by defining principles and procedures for maintaining the privacy and security of sensitive information. It also ensures that all employees, trustees, contractors, volunteers, and stakeholders understand their responsibilities regarding the handling, protection, and disclosure of information.

2. What is confidentiality?

Confidentiality is about safeguarding information that is private, sensitive, or marked as restricted and ensuring it is not shared with anyone who is not authorised to access or know about it. These includes employee personal details, business strategies, commercial information, residents' information, trade secrets, and any other data considered confidential. Confidentiality means respecting a person's right to keep their information private unless they choose to share it.

Whenever it's appropriate to share personal information, it should only be done with the individual's explicit consent. Our Data Protection Policy provides guidance on when personal data may be disclosed and should be read alongside this policy. Protecting confidentiality fosters trust, which is vital for individuals on behalf of the Trust to confidently share information and raise concerns when required.

3. Confidentiality and Data Protection.

This policy aligns with applicable data protection laws and regulations, such as the General Data Protection Regulation (GDPR) 2018, the Privacy and Electronic Communications Regulations (PECR) etc. Personal data must be processed lawfully, fairly, and transparently, always ensuring confidentiality, accuracy, and integrity.

4. Who does it apply to?

This policy applies to all trustees, employees, residents, contractors, consultants, volunteers, and any other individuals who have access to confidential information belonging to or held by Retail Trust. Retail Trust shall always act to protect the rights of individuals by ensuring that all individuals likely to be affected by our Data Protection Policy are aware of the principles and procedures involved.

5. Collection and storage of information?

Confidential information should only be collected and stored for legitimate business purposes. It must be:

- obtained and used lawfully, fairly and in a transparent manner;
- collected and held for specific, explicit, and legitimate purposes and only used for those purposes;
- adequate, relevant, and limited to what is necessary for our purposes;
- kept no longer than necessary and destroyed (using a secure method) when no longer required;
- stored securely using encryption or other appropriate measures.
- accessed only by authorised individuals.
- regularly reviewed and updated to ensure accuracy and necessity.

6. Limits to Confidentiality.

There may be cases when the Trust is required to share information with relevant parties. This could be due to a duty of care, where an issue must be addressed, or a legal obligation to disclose information.

Such requirements typically fall into two categories: responding to specific requests for information on a case-by-case basis or proactively reporting information when it comes to your attention.

Instances where information may be disclosed without prior consent of the individual are:

- when disclosure is required by law (e.g., court orders, subpoenas, Police, benefits agencies, etc).
- in cases where there is a risk of harm to self or others (health and safety risk).
- to comply with regulatory or statutory obligations.
- where information is required for statistical purposes or research, provided it is not possible to identify the individuals to whom the information relates.
- to enable contractors to make arrangements for access to provide services on the Trust's behalf (only if this has been set out in a privacy notice to the individual);

The Data Protection Policy sets out requirements for "privacy notices", which include information regarding disclosure of personal data to third parties and where individuals must be informed of such disclosure.

7. Access to Information.

Access to confidential information is restricted to individuals on a "need to know" basis. Unauthorised access, even within the organisation, is strictly prohibited. Where information is to be shared between departments or with external agencies, such information must be shared via secured shared folder and must ensure that the individual's written agreement is obtained before any information is shared.

8. Your Role.

Every individual covered under this policy has a duty to:

- understand and adhere to confidentiality requirements.
- ensure the secure handling of confidential information.
- report breaches or suspected breaches of confidentiality promptly.

Everyone is obligated to maintain their own confidentiality. You should be clear when you are talking to other people on whether what you are saying is confidential or not.

9. Use of AI.

The Trust may use Artificial Intelligence (AI) tools to process, analyse, or manage confidential information. Any use of AI must comply with this confidentiality policy, Retail Trust internal Responsible AI Policy and relevant data protection laws. Employees must:

- ensure AI tools are vetted and approved by the relevant department.
- avoid inputting sensitive or confidential information into unauthorised AI platforms.
- monitor AI outputs for accuracy and confidentiality.

10. What Happens if I Lose or Mistakenly Disclose Confidential Information?

If confidential information is lost or disclosed in error, the incident must be reported immediately to your line manager who must forward all the incident details immediately to the Data Protection Team via dataprotection@retailtrust.org.uk . An investigation will be conducted to determine the cause and mitigate potential damage. Consequences for the individual responsible will depend on the severity of the breach.

11. Maintaining Confidentiality

To maintain confidentiality:

- do not discuss sensitive information in public or unsecured environments.
- use secure methods for sharing information (e.g., encrypted emails).

- ensure that, where possible, confidential telephone conversations cannot be overheard.
- ensure that you lock your workstation when leaving your desk.
- ensure that you print documents using the secure settings mode.
- passwords protect any USB devices you use for work.
- ensure confidential paperwork is put away when you leave your desk.
- do not leave any keys out which may allow access to files or documents.
- do not discuss personal details about another person with someone else unless that information is required.
- lock any drawers/storage areas that you may use before leaving your work area.
- password protect any files containing sensitive information before you attach them to an email which you are sending externally/internally.
- external clients or visitors to the Charity's premises should always be accompanied and not left unattended. They must sign in and wear a clearly visible visitor badge.
- personal data should be securely stored, such as in a locked filing cabinet, to ensure its protection.
- any written confidential documents that are no longer needed must be shredded in accordance with our Data Retention Policy.
- information about residents, service users, clients, or staff should not be shared with others, including advocates, unless they are authorised to receive such information.

While it is encouraged that staff show concern for one another's well-being, no one should feel obligated to disclose information about a colleague's absence or personal matters, except when required for official HR or payroll purposes.

12. Non-Compliance.

Failure to comply with this policy may result in disciplinary action, including termination of employment or contractual agreements. Legal action may also be pursued in cases of severe or intentional breaches.