

FOOTSTEPS TRUST DATA PROTECTION AND INFORMATION GOVERNANCE POLICY

1. Policy Statement

Footsteps Trust Academy is committed to protecting the privacy, confidentiality, integrity and availability of personal information.

The Academy processes personal information relating to:

- Students
- Parents and carers
- Staff
- Trustees
- Volunteers
- Referrers and commissioning bodies
- Contractors
- Visitors

The Academy recognises that effective information governance supports safeguarding, education, welfare and operational effectiveness.

This policy sets out how personal information is collected, used, stored, shared and disposed of in accordance with UK data protection legislation.

2. Legislative Framework

This policy has regard to:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Freedom of Information Act 2000
- Human Rights Act 1998
- Keeping Children Safe in Education 2026
- Independent School Standards
- Working Together to Safeguard Children

The Academy will ensure that information handling supports its safeguarding responsibilities and protects the rights of individuals.

3. Data Protection Principles

When processing personal data, Footsteps will ensure information is:

- **Lawful, Fair and Transparent** - Data will only be processed using an appropriate lawful basis.
- **Collected for Specified Purposes** - Information will only be used for legitimate educational, safeguarding, operational or legal purposes.
- **Adequate, Relevant and Limited** - Only information necessary for the specified purpose will be collected.
- **Accurate and Up to Date** - Reasonable steps will be taken to maintain accurate records.
- **Kept Only as Long as Necessary** - Retention schedules will be followed.
- **Secure** - Appropriate technical and organisational measures will be implemented to protect information.
- **Accountable** - The Academy will demonstrate compliance with UK GDPR requirements.

4. Categories of Information Processed

The Academy may process:

Student Information

Including:

- Admission details
- Educational records
- Attendance information
- SEND information
- Behaviour records
- Safeguarding records
- Medical information
- Assessment and examination data

Workforce Information

Including:

- Recruitment records
- Payroll information
- Training records
- Performance information
- DBS information

Parent and Carer Information

Including:

- Contact details

Date of Issue: September 2026

Date of Review: September 2027

- Emergency contacts
- Communications records

Contractor and Visitor Information

Where necessary for operational and safeguarding purposes.

5. Special Category Data

The Academy may process special category data relating to:

- Health
- Disability
- Ethnicity
- Religion or belief
- Biometric information (where applicable)
- Safeguarding concerns

Such information will only be processed where lawful and necessary and with appropriate safeguards in place.

6. Information Sharing

The Academy recognises that effective information sharing is essential to safeguarding.

Information may be shared with:

- Local Authorities
- Social Care
- Police
- Health Professionals
- Other Educational Settings
- Alternative Provision Commissioners
- Regulators
- Examination Bodies

Information will only be shared where:

- There is a lawful basis.
- Sharing is necessary and proportionate.
- Safeguarding responsibilities require it.
- Consent has been obtained where appropriate.

Where safeguarding concerns exist, the welfare of the child will take precedence.

7. Safeguarding Records

Child protection and safeguarding records require enhanced protection.

The Academy will:

- Restrict access to authorised staff.
- Store records securely.
- Transfer records securely when students move settings.
- Maintain confidentiality.
- Retain records in accordance with safeguarding requirements.

Safeguarding information may be shared without consent where necessary to protect a child from harm.

8. Cyber Security and Information Security

To protect personal information, the Academy will maintain:

- Secure networks.
- Firewall protection.
- Endpoint security.
- Multi-factor authentication where appropriate.
- Data encryption.
- Access controls.
- Secure cloud systems.
- Filtering and monitoring arrangements.
- Cyber security training.

Staff must immediately report any suspected security incident or data breach.

9. Data Retention and Disposal

The Academy will maintain a separate Data Retention Schedule.

Information will:

- Be retained only as long as necessary.
- Be reviewed regularly.
- Be securely destroyed when retention periods expire.

Electronic data will be permanently deleted where appropriate and paper records securely shredded.

10. Data Subject Rights

Individuals have the right to:

- Be informed.
- Access their information.
- Request correction of inaccurate information.
- Request deletion in certain circumstances.
- Restrict processing.
- Object to processing.
- Request portability where applicable.
- Complain to the Information Commissioner's Office (ICO).

The Academy will respond to rights requests within statutory timescales.

11. Subject Access Requests (SARs)

Requests may be made verbally or in writing.

The Academy will:

- Verify identity.
- Record the request.
- Respond within one calendar month unless an extension is permitted by law.
- Consult the Data Protection Officer where required.

Detailed SAR procedures are contained within Appendix A.

12. Data Breaches

A personal data breach may include:

- Unauthorised disclosure.
- Loss of personal information.
- Cyber attack.
- Accidental deletion.
- Unauthorised access.

All breaches must be reported immediately to:

- The Principal
- Data Protection Lead
- Data Protection Officer

The Academy will investigate breaches and report them to the ICO where legally required.

13. Data Protection Impact Assessments (DPIAs)

The Academy will conduct DPIAs where processing is likely to result in a high risk to individuals.

Examples include:

- New software systems.
- Large-scale processing.
- Monitoring technologies.
- CCTV expansion.
- New safeguarding technologies.

DPIAs will identify and mitigate privacy risks before implementation.

14. Staff Responsibilities

All staff must:

- Complete data protection training.
- Follow Academy policies.
- Protect confidential information.
- Use secure systems.
- Report breaches immediately.
- Follow retention and disposal procedures.

Failure to comply with this policy may result in disciplinary action.

15. Data Protection Officer (DPO)

The Academy appoints an independent Data Protection Officer to:

- Monitor compliance.
- Provide advice and guidance.
- Support data protection impact assessments.
- Assist with data subject rights requests.
- Liaise with the ICO.

The Academy should update the DPO details annually to ensure accuracy.

16. Equality and Accessibility

The Academy will ensure that:

- Privacy information is accessible.
- Subject Access Requests can be made by all individuals.
- Reasonable adjustments are provided where required.
- Children's evolving capacity and rights are considered appropriately.

This is particularly important when handling requests relating to safeguarding and vulnerable learners.

17. Monitoring and Review

The Principal, DPO and Trustees will monitor:

- Data breaches.
- Compliance audits.
- Subject Access Requests.
- Training completion.
- Security incidents.
- Policy effectiveness.

The policy will be reviewed annually or in response to legislative changes, ICO guidance updates or significant incidents.

Appendix 1 – Subject Access Requests

Under Data Protection Law, Data Subjects have a general right to find out whether Footsteps hold or process personal data about them, to access that data, and to be given supplementary information. This is known as the right of access, or the right to make a data subject access request (SAR). The purpose of the right is to enable the individual to be aware of, and verify, the lawfulness of the processing of personal data that Footsteps are undertaking.

A Data Subject has the right to be informed by Footsteps of the following: -

- (a) Confirmation that their data is being processed;
- (b) Access to their personal data;
- (c) A description of the information that is being processed;
- (d) The purpose for which the information is being processed;
- (e) The recipients/class of recipients to whom that information is or may be disclosed;
- (f) Details of Footsteps' sources of information obtained;



(g) In relation to any Personal Data processed for the purposes of evaluating matters in relation to the Data Subject that has constituted or is likely to constitute the sole basis for any decision significantly affecting him or her, to be informed of the logic of the Data Controller's decision making. Such data may include, but is not limited to, performance at work, creditworthiness, reliability and conduct; and

(h) Other supplementary information.