



GDPR POLICY

JUNE 2026

Policy Date: June 2026
Review Cycle: Annually
Responsible Body: Trust Board

Version Control

Review Date	Updates
V1 September 2025	Initial drafting
V2 April 2026	Update - biometric data
V3 June 2026	Updated legislation requirements

Contents

Contents	2
Policy	3
Aims	3
Legal Framework	3
Definitions	4
Roles and Responsibilities	4
Data Protection Principles	5
Individual Rights	5

Policy

Spark Education Trust is committed to ensuring that all personal data relating to pupils, parents and carers, employees, trustees, governors, volunteers, visitors and other individuals is collected, stored and processed in accordance with applicable data protection legislation.

The Trust recognises its responsibilities as a data controller and is committed to maintaining the highest standards of information governance, confidentiality and data security across all academies and central services.

This policy applies to all personal data processed by Spark Education Trust and all schools within the trust regardless of whether the information is held electronically or in paper format.

Aims

The aims of this policy are to:

- Ensure compliance with all relevant data protection legislation.
- Protect the rights and freedoms of individuals whose personal data is processed by the Trust.
- Establish clear responsibilities for the management and protection of personal data.
- Promote good practice in the collection, use, retention and disposal of personal data.
- Ensure personal data is processed lawfully, fairly and transparently.
- Minimise the risk of personal data breaches and ensure appropriate action is taken where breaches occur.

Legal Framework

This policy meets the requirements of:

- UK General Data Protection Regulation (UK GDPR).
- Data Protection Act 2018.
- Data (Use and Access) Act 2025.
- Protection of Freedoms Act 2012 (where biometric data is processed).

This policy is informed by guidance published by the Information Commissioner's Office (ICO) and the Department for Education (DfE). This policy also complies with the Trust's Funding Agreement and Articles of Association.

Definitions

Term	Definition
Personal Data	Any information relating to an identified or identifiable living individual.
Special Category Data	Personal data requiring additional protection, including information relating to racial or ethnic origin, political opinions, religious beliefs, trade union membership, genetics, biometrics, health, sex life or sexual orientation.
Processing	Any activity involving the collection, storage, use, sharing, amendment or deletion of personal data.
Data Subject	The individual whose personal data is processed.
Data Controller	The organisation that determines the purposes and means of processing personal data.
Data Processor	A person or organisation that processes personal data on behalf of the data controller.
Personal Data Breach	A breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

Roles and Responsibilities

Role	Responsibility
Trust Board	Has overall responsibility for ensuring compliance with data protection legislation.
Data Protection Officer (DPO)	Responsible for monitoring compliance with data protection legislation and providing advice and support to the Trust. Data Protection Officer Contact Details: Natasha Yeronimou Email: dpo@sparkeducation.org.uk
Chief Executive Officer and Headteachers	Responsible for the day-to-day implementation of this policy within their areas of responsibility.
Director of IT	Responsible for supporting the implementation of appropriate technical and organisational security measures.

Data Protection Principles

Spark Education Trust will ensure that personal data is:

- Processed lawfully, fairly and transparently.
- Collected for specified, explicit and legitimate purposes.
- Adequate, relevant and limited to what is necessary.
- Accurate and kept up to date where necessary.
- Retained only for as long as necessary.
- Processed securely and confidentially.
- Transferred internationally only where appropriate safeguards exist.
- Processed in a manner that upholds the rights of individuals.
- Processed in accordance with the accountability principle.

Collection and Processing of Personal Data

The Trust will only process personal data where a lawful basis exists under data protection legislation. The Trust will ensure that personal data is collected only for legitimate purposes, processed fairly and transparently, and retained only for as long as necessary. Individuals will be provided with appropriate privacy information explaining how their personal data is collected and used via the Trust Privacy Notice.

Sharing Personal Data

The Trust will only share personal data where there is a lawful basis to do so and where appropriate safeguards are in place. Information may be shared where required by law, for safeguarding purposes, to support the education and wellbeing of pupils or to enable contracted services to be provided. Where third-party organisations process personal data on behalf of the Trust, appropriate written contracts and data processing agreements will be in place.

Individual Rights

Individuals have rights under data protection legislation including:

- The right to be informed.
- The right of access.
- The right to rectification.
- The right to erasure.
- The right to restrict processing.
- The right to object.
- Rights relating to automated decision-making.
- The right to lodge a complaint with the Information Commissioner's Office.

Requests relating to these rights should be directed to the Data Protection Officer.

Educational Records

The Trust will respond to requests for access to educational records in accordance with applicable legislation and guidance.

Subject Access Requests

The Trust will respond to requests for access to personal data in accordance with statutory timescales and legal requirements.

Biometric Recognition Systems

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use fingerprints to take payment for school dinners instead of cash, we will comply with the requirements of the Protection of Freedoms Act 2012 and the UK GDPR.

Parents and carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at least 1 parent or carer before we take any biometric data from their child and first process it.

Parents and carers and pupils have the right to choose not to use the school's biometric system. We will provide alternative means of accessing the relevant services for those pupils.

Parents and carers and pupils can withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parents/carers.

CCTV and Surveillance Systems

The Trust operates CCTV systems to support safeguarding, security and crime prevention. All CCTV systems will operate in accordance with applicable legislation and ICO guidance.

Photographs and Videos

The Trust may take photographs and videos as part of activities within Trust schools. Appropriate consent will be obtained where required and individuals may withdraw consent at any time.

Artificial Intelligence (AI)

The Trust recognises the opportunities presented by artificial intelligence technologies whilst also recognising the importance of protecting personal and sensitive information. Personal information must only be processed using approved systems and in accordance with data protection requirements.

The Trust will implement appropriate technical and organisational measures to protect personal data from unauthorised access, loss, misuse or disclosure.

Personal Data Breaches

The Trust will take all reasonable steps to prevent personal data breaches. Where a breach occurs, it will be managed in accordance with Trust procedures and legal requirements. The Trust will ensure that appropriate data protection training and awareness is provided to staff and relevant stakeholders. Where required by law, the Trust will report personal data breaches to the Information Commissioner's Office and affected individuals within the statutory timescales.

Complaints

Complaints will be handled in line with the Data (Use and Access) Act 2025. Complaints regarding the processing of personal data can be submitted to the Data Protection Officer at dpo@sparkeducation.org.uk. Individuals also have the right to complain to the Information Commissioner's Office.

We will acknowledge receipt of complaints within 30 days of receiving them and without undue delay. We will take appropriate steps to respond to complaints, including making appropriate enquiries, keeping the complainant informed and notifying the complainant of the outcome of their complaint.

Individuals should ordinarily raise concerns with the Trust before referring matters to the Information Commissioner's Office.

Related Policies

This policy should be read alongside relevant Trust policies including:

- Privacy Notice
- Freedom of Information Publication Scheme
- Online Safety Policy
- ICT Acceptable Use Policy
- Safeguarding and Child Protection Policy
- Staff Code of Conduct

Personal data will be retained and disposed of in accordance with the Trust's records retention arrangements and applicable statutory retention requirements.