



Data Protection Policy

We Care • We Challenge • We Commit

Document Control Table			
Document Title:	Data Protection Policy		
Owner:	Dunstone Education Trust		
Approved on:	September 2022		
Author Name:			
Version	V4		
Approved by:	Dunstone Trust Board		
Review date:	September 2026		
Document History:			
Version	Date	Author	Note of revisions
V1	Sept 2022		Adoption of Policy
V1	Sept 2023		No revisions required
V2	Sept 2024		Change made to DPO
V3	Sept 2025		Full update for DUAA 2025, DfE AI guidance
V4	Sept 2026		Updated document control table, review cycle, linked governance wording, and alignment with current DfE data protection guidance for schools. Section 5: Collecting and Using Personal Data — added wording on privacy notices. Section 7: Sharing Personal Data — added wording on necessity, proportionality and recording requirements. Section 8: SARs and Individual Rights — softened the wording on children’s subject access requests and added a complaints process. Section 11: CCTV — added a cross-reference to photographs, videos and CCTV guidance. Section 12: Photographs and Videos — expanded the section to cover purpose, lawful basis, retention and use of personal devices. Section 13: AI and Data Protection — rewrote the section to provide more precise wording on AI use and data protection requirements. Section 14: Data Protection by Design and Default — added wording on records of processing activities. Section 15: Data Security — strengthened wording on cyber security controls. Section 16: Data Breaches — changed references from IC to ICO and clarified the 72-hour reporting requirement. Section 19: Links with Other Policies — added missing linked documents.

--	--	--	--

Mission Statement

We promote a culture of educational excellence, kindness, and respect within our school and wider community. Our core values are: **We Care, We Challenge, We Commit**. These guide how we handle everyone's personal information safely and responsibly.

1. Introduction and Background

Dunstone Education Trust collects, stores, and processes personal data about staff, pupils, parents, governors, visitors, and others. We comply with:

- The Data (Use and Access) Act 2025 (DUAA)
- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Information Commission guidance
- Keeping Children Safe in Education (KCSIE) 2025
- DfE Guidance on AI and Data Protection (2025)

This policy applies to all personal data, in any format.

2. Definitions

- Personal data: Information relating to an identified or identifiable individual (e.g. name, ID, location, online identifiers).
- Special categories of personal data: Sensitive data needing extra protection (e.g. health, ethnicity, beliefs, genetics, biometrics).
- Processing: Any action involving personal data (e.g. collecting, storing, sharing, deleting).
- Data subject: The individual the data is about.
- Data controller: The person/organisation deciding why and how data is processed (the Trust).
- Data processor: Anyone processing data on behalf of the Trust.
- Personal data breach: Accidental or unlawful loss, destruction, alteration, unauthorised disclosure, or access to data.

3. Roles and Responsibilities

- Trust Board: Overall responsibility for data protection.

- Data Protection Officer (DPO): Oversees policy implementation, monitors compliance, provides advice, and is first point of contact for concerns.
DPO contact: Mrs. Livesey — d.livesey@fulwoodacademy.co.uk
- All staff and contractors: Must comply with this policy and attend regular training.

4. Data Protection Principles

Personal data must be:

1. Processed lawfully, fairly, and transparently.
2. Collected for specified, explicit, and legitimate purposes.
3. Adequate, relevant, and limited to what is necessary.
4. Accurate and kept up to date.
5. Kept for no longer than necessary.
6. Processed securely.

5. Collecting and Using Personal Data

We process personal data only when we have a legal reason (lawful basis), such as:

- Fulfilling a contract (e.g. staff employment)
- Meeting a legal obligation
- Protecting someone's vital interests
- Performing a task in the public interest
- Legitimate interests of the Trust (balanced with individual rights)
- Clear consent (where needed)

We provide clear information about what data we collect, why, and how it will be used. For children under 13, parental consent is required for most online services.

Privacy notices

The Trust will maintain clear, accessible and up-to-date privacy notices explaining how personal data is collected, used, shared, retained and protected. Privacy notices will be made available to relevant groups, including pupils, parents and carers, staff, job applicants, governors, trustees, volunteers, visitors, suppliers and other individuals whose personal data is processed by the Trust.

Privacy notices will be reviewed at least annually, and sooner where there are significant changes to legislation, guidance, systems, suppliers, data sharing arrangements, use of AI tools, or the purposes for which personal data is processed.

6. Limiting, Minimising, and Ensuring Accuracy

- Only collect and use data needed for the specified purpose.

- Staff only process data needed for their work.
- Data is deleted or anonymised when no longer needed, following our retention schedule.
- If we need to use data for a new purpose, we inform individuals and seek consent if required.

7. Sharing Personal Data

We will not usually share personal data, except when:

- There is a safeguarding or safety risk.
- Other agencies need it for their statutory duties.
- Contractors need it to deliver services (under strict agreements).
- Required by law (e.g. police, HMRC, courts).
- Emergency services need information to protect pupils or staff.
- Data is anonymised for research/statistics.

International transfers: Data sent outside the UK/EEA is protected according to law.

Before sharing personal data, staff must consider whether the sharing is lawful, fair, necessary and proportionate. Where appropriate, the Trust will record the purpose of the sharing, the lawful basis relied upon, what information was shared, with whom it was shared, and any relevant safeguarding, statutory or public interest reason. Consent is not always required to share personal data, particularly where sharing is necessary for safeguarding, statutory duties, legal obligations, vital interests, or the performance of a public task. However, staff must not share more information than is necessary for the purpose.

8. Subject Access Requests (SARs) and Individual Rights

Data (Use and Access) Act 2025 update:

- We carry out a “reasonable and proportionate” search for SARs.
- We keep a record of steps taken and reasons for any limitations.

Individuals have the right to:

- Request access to their data (SAR)
- Correct, erase, or restrict processing
- Withdraw consent
- Object to processing
- Prevent direct marketing
- Request data transfer (where applicable)
- Challenge automated decisions

SAR process:

- Requests are acknowledged within 1 month (or up to 3 months if complex).
- ID may be requested.
- Requests may be refused if excessive, repetitive, or unfounded (with reasons given).
- The Information Commission (IC) is the complaints authority.

Children's SARs:

Children 12+ usually manage their own data. Parents/carers can request only if the child cannot understand or has given permission.

Data protection complaints

Individuals may raise a complaint with the Trust if they are concerned about how their personal data has been collected, used, shared, retained, or otherwise processed. Complaints should be directed to the Data Protection Officer in the first instance. The Trust will acknowledge and investigate complaints promptly, keep appropriate records, and provide a clear response explaining the outcome and any action taken.

Requests relating to children's personal data will be considered on a case-by-case basis, taking into account the child's age, maturity, understanding and best interests. Where a child is considered capable of understanding their data protection rights, the Trust will usually respond directly to the child unless they have authorised a parent or carer to act on their behalf, or there is another lawful basis for disclosure.

Where an individual remains dissatisfied, they may contact the Information Commissioner's Office. The Trust will keep this complaints process under review and update it in line with any commencement regulations or guidance issued under the Data (Use and Access) Act 2025.

9. Safeguarding and Data Protection

KCSIE 2025:

Data protection law does not prevent information sharing where there is a risk of serious harm to a child or others. Safeguarding always comes first.

10. Data Audits, Retention, and Disposal

- We audit all data we hold (paper, digital, AI platforms, CCTV, etc.) at least annually.
- We keep data only as long as needed, as set out in our retention schedule.
- Unnecessary/outdated data is deleted securely (shredded, incinerated, or digitally wiped).
- Third parties disposing of data must guarantee compliance.

11. CCTV

- CCTV is used for safety.
- Cameras are signposted and obvious.
- Enquiries: Mr. Hedingham — m.hedingham@fulwoodacademy.co.uk

12. Photographs and Videos

- Written consent is required from parents/carers or pupils aged 18+ for most uses.
- Pupils/parents can withdraw consent at any time.
- Photos/videos for publicity never include personal info.
- Consent and usage are clearly explained up front.

The Trust will distinguish between images or recordings used for internal educational, safeguarding, identification, operational, security, publicity and media purposes. The lawful basis and consent requirements may differ depending on the purpose. Staff must only take, store, use or share photographs and videos in accordance with Trust procedures, privacy notices, consent records and safeguarding expectations.

Images and recordings must be stored securely, retained only for as long as necessary, and deleted when no longer required. Staff must not use personal devices to capture or store pupil images unless specifically authorised by senior leadership and subject to appropriate safeguards.

13. AI and Data Protection

DfE AI Guidance 2025:

- Only use AI tools after Data Protection Impact Assessment (DPIA).
- AI vendors must show compliance with UK GDPR and DUAA.
- Data Processing Agreements (DPA) required for all AI suppliers.
- Parents/carers informed of any AI use processing pupil data.
- Staff trained in secure AI use and risks.
- Any use of special category data in AI systems is subject to extra safeguards.

AI and Data Protection

The Trust recognises that artificial intelligence tools may create specific risks for privacy, confidentiality, safeguarding, accuracy, fairness, transparency and security. AI tools must not be used to process personal data unless they have been approved through the Trust's agreed assessment process.

Where the proposed use of AI involves personal data, pupil data, staff data, special category data, safeguarding information, automated decision-making, profiling, monitoring, or any processing that may create a high risk to individuals, the Trust will complete a Data Protection Impact Assessment before the tool is introduced. Staff must not enter personal data, confidential school information, safeguarding information, assessment information, health information, special category data, or any information that could identify a pupil, parent, carer,

member of staff or other individual into a public or unapproved AI tool.

Any AI supplier used by the Trust must be subject to appropriate due diligence, contractual controls, data processing terms, security review and, where required, a Data Processing Agreement. The Trust will ensure that parents, carers, pupils and staff are provided with appropriate information where AI tools are used to process their personal data. AI outputs must be checked by an appropriate member of staff before use. AI must not be used as the sole basis for decisions that have a legal, safeguarding, disciplinary, educational or similarly significant effect on an individual unless this has been specifically assessed, approved and communicated in accordance with data protection law.

14. Data Protection by Design and Default

- DPO ensures privacy is embedded in all processes and technologies.
- Data protection impact assessments (DPIAs) carried out for new tech and high-risk activities.
- Internal records kept of all data processing, storage, and sharing.
- All related policies and privacy notices are kept up to date.
-

The Trust will maintain appropriate records of processing activities, including the categories of personal data processed, the purposes of processing, lawful bases, categories of data subjects, data sharing arrangements, retention periods, security measures, systems used, processors, and any international transfers. These records will be reviewed regularly and updated when new systems, suppliers, processes or purposes are introduced.

15. Data Security

- Personal data is protected against unauthorised access, loss, alteration, or disclosure.
- Paper and devices are locked away when not in use.
- Passwords are strong, regularly updated.
- Encryption is used for portable devices.
- Personal info must not be stored on personal devices without approval.
- Third parties must meet our security requirements.

The Trust will apply appropriate technical and organisational measures to protect personal data. These may include role-based access controls, multi-factor authentication where appropriate, secure password practices, encryption, secure configuration, regular software updates, secure backups, audit logs, staff training, supplier assurance, secure disposal, and incident response arrangements.

Access to personal data will be limited to staff and authorised users who need it for their role. Access permissions will be reviewed regularly and removed promptly when staff leave the Trust or change role.

16. Data Breaches

- All staff report suspected breaches immediately to the DPO.
- The DPO logs all breaches and reports to the Information Commission (IC) within 72 hours where required.
- Breaches involving safeguarding or AI tools are handled according to KCSIE and DfE guidance.
- Procedures for handling breaches are outlined in the Data Breach Policy.

17. Training

- All staff receive data protection training annually, including DUAA, KCSIE, and DfE AI requirements.
- Training records are kept and reviewed.

18. Monitoring and Review

- The DPO reviews this policy every year and after any major legal or guidance update.
- Policy is approved by the Trust Board and shared with all staff.

19. Links with Other Policies

19. Links with Other Policies

This policy should be read alongside the Trust's:

- Subject Access Request Policy
- Records Management and Retention Schedule
- Privacy Notices
- Data Breach Policy
- Safeguarding and Child Protection Policy
- Acceptable Use Policy
- Information Security Policy
- CCTV Policy
- Online Safety Policy
- AI Use Procedure
- Staff Code of Conduct
- Freedom of Information Policy, where applicable

Contact the Data Protection Officer with any questions or concerns about this policy or about the handling of personal data.

Contact the DPO with any questions or concerns about this policy or your personal data.

