



DATA MANAGEMENT POLICY

2026-2027

OWNERSHIP: Everything Education School

AUTHORISED BY: M Hussain (Headteacher)

EFFECTIVE FROM: 11/9/2026

REVIEW: 11/9/2027

Everything Education School

1234-1238 Coventry Road, Yardley, Birmingham B25 8BZ

CONTENTS

1.0 Purpose and Scope.....	3
2.0 Legal and Regulatory Framework.....	3
3.0 Data Protection Principles.....	3
4.0 Roles and Responsibilities.....	3
5.0 Categories and Sources of Personal Data.....	3
6.0 Lawful Bases and Special Category Data.....	4
7.0 Privacy Information and Transparency.....	4
8.0 Data Sharing and Third Parties.....	4
9.0 Information Security.....	4
10.0 Artificial Intelligence, Digital Services and EdTech.....	4
11.0 Data Protection Impact Assessments.....	4
12.0 Retention and Secure Disposal.....	4
13.0 Individual Rights and Subject Access Requests.....	5
14.0 Data Breaches.....	5
15.0 Data Protection Complaints and Concerns.....	5
16.0 Training, Audit and Compliance Monitoring.....	5
17.0 Records and Documentation.....	5
18.0 Review of This Policy.....	5
Related Guidance.....	5

1.0 PURPOSE AND SCOPE

Everything Education School collects and uses personal information about pupils, parents and carers, staff, applicants, commissioners, professionals, suppliers and other individuals connected with the school. This policy sets out how personal data must be collected, used, shared, stored, retained and disposed of lawfully, fairly, transparently and securely.

The policy applies to personal data in any format, including electronic systems, email, cloud services, paper records, photographs, video, CCTV where used, audio recordings and information processed through approved digital or artificial intelligence (AI) tools.

2.0 LEGAL AND REGULATORY FRAMEWORK

The school will comply with applicable UK data protection law and relevant education guidance, including:

- UK General Data Protection Regulation (UK GDPR).
- Data Protection Act 2018.
- Data (Use and Access) Act 2025, which amends and supplements the UK data protection framework.
- Privacy and Electronic Communications Regulations (PECR), where applicable.
- Department for Education (DfE) guidance on data protection in schools and Information Commissioner's Office (ICO) guidance.

3.0 DATA PROTECTION PRINCIPLES

Personal data must be handled in accordance with the seven UK GDPR principles. The school will ensure that personal data is:

1. Lawfulness, fairness and transparency: processed lawfully, fairly and in a transparent manner.
2. Purpose limitation: collected for specified, explicit and legitimate purposes and not used incompatibly with those purposes.
3. Data minimisation: adequate, relevant and limited to what is necessary.
4. Accuracy: accurate and, where necessary, kept up to date.
5. Storage limitation: kept in identifiable form for no longer than necessary, subject to lawful retention requirements.
6. Integrity and confidentiality: protected by appropriate technical and organisational security measures.
7. Accountability: managed so that the school can demonstrate compliance with these principles.

4.0 ROLES AND RESPONSIBILITIES

Everyone who works for or on behalf of Everything Education School is responsible for protecting personal data and must follow this policy, associated procedures and staff training.

Data Protection Lead / DPO: Madausr Hussain.

The Data Protection Lead/DPO will oversee compliance, advise the school on data protection matters, maintain appropriate records, support data protection impact assessments (DPIAs), coordinate staff training, advise on data breaches and individual rights requests, and act as a point of contact with the ICO where required.

The proprietor body and school leadership will ensure that sufficient resources, systems and oversight are in place to support compliance. Staff must immediately report any suspected loss, disclosure, misuse or unauthorised access to personal data.

5.0 CATEGORIES AND SOURCES OF PERSONAL DATA

Depending on the purpose, the school may process:

- identification and contact information, including names, addresses, dates of birth, telephone numbers and email addresses;
- pupil education records, assessment information, attainment, attendance, behaviour, timetables, destinations and provision information;
- special category data, including information about health, disability/SEND, ethnicity, religion where relevant, and safeguarding or welfare information;
- criminal offence information where there is a lawful basis and appropriate condition for processing;
- parent/carers, staff, contractor, volunteer, visitor and commissioner information;
- online identifiers, account and access information, and audit/security logs;
- photographs, video, CCTV or recordings where used for an identified lawful purpose.

Data may be obtained directly from individuals or from schools, local authorities, commissioners, parents/carers, health or social care professionals, previous settings, alternative provisions, examination bodies and other organisations where sharing is lawful and necessary.

6.0 LAWFUL BASES AND SPECIAL CATEGORY DATA

The school will identify and record an appropriate lawful basis for each processing activity. Depending on the activity, this may include legal obligation, public task, contract, vital interests, legitimate interests or consent. Consent will not be used where another lawful basis is more appropriate or where an individual does not have a genuine choice.

Where special category or criminal offence data is processed, the school will identify the additional condition required by law and maintain any necessary safeguards or policy documentation. Safeguarding information may be shared without consent where this is lawful and necessary to protect a child or another person from harm.

7.0 PRIVACY INFORMATION AND TRANSPARENCY

The school will provide clear privacy information explaining what information is collected, why it is used, the lawful basis, who it may be shared with, how long it is retained, relevant individual rights, and how to raise a concern. Privacy notices will be reviewed when processing changes or when legislation or guidance is updated.

8.0 DATA SHARING AND THIRD PARTIES

Personal data will only be shared where there is a clear lawful basis and the disclosure is necessary, proportionate and secure. This may include sharing with local authorities and commissioners, schools, safeguarding partners, health and social care services, examination bodies, regulators, professional advisers, law enforcement or other recipients where permitted or required by law.

Where an external organisation processes personal data on the school's behalf, the school will carry out proportionate due diligence and put an appropriate written data processing agreement or contract in place. Staff must use approved secure channels and must not use personal email accounts or unapproved applications to share school information.

9.0 INFORMATION SECURITY

The school will apply appropriate technical and organisational measures based on risk. These include, where appropriate:

- role-based access controls and the principle of least privilege;
- multi-factor authentication and strong password controls;
- encryption for devices, storage and transfers where appropriate;
- approved secure cloud services and restricted sharing links;
- device locking, software updates, anti-malware, filtering/monitoring and secure backups;
- secure storage and confidential destruction of paper records;
- staff training, confidentiality expectations and regular review of access rights.

10.0 ARTIFICIAL INTELLIGENCE, DIGITAL SERVICES AND EDTECH

Staff must only use AI, EdTech and digital services approved by the school for school business. Before personal data is entered into a new system or AI service, the school will consider the lawful basis, transparency, security, supplier terms, international transfers, retention, age-appropriateness and whether a DPIA is required. Personal or special category pupil data must not be entered into public or unapproved generative AI services.

11.0 DATA PROTECTION IMPACT ASSESSMENTS

A DPIA will be completed before high-risk processing begins, including where new technology or large-scale/sensitive processing is likely to result in a high risk to individuals. The DPIA will identify the purpose, necessity, risks and measures to reduce those risks. The Data Protection Lead/DPO will be consulted as part of this process.

12.0 RETENTION AND SECURE DISPOSAL

Personal data will be kept only for as long as there is a lawful and operational need, taking account of statutory, safeguarding, education, employment, contractual and limitation requirements. The school will maintain or adopt a retention schedule and will review records regularly. When records are no longer required, they will be securely deleted, anonymised or confidentially destroyed.

13.0 INDIVIDUAL RIGHTS AND SUBJECT ACCESS REQUESTS

Individuals have rights under data protection law, subject to conditions and exemptions. These include rights to be informed, access personal data, rectification, erasure in certain circumstances, restriction, data portability where applicable, objection, and rights relating to certain automated decision-making.

A request for access to personal data does not have to use a particular form. Staff who receive a request must send it promptly to the Data Protection Lead/DPO. The school will verify identity where necessary, identify the relevant information, consider third-party information and applicable exemptions, and respond within the statutory timeframe. Requests concerning children will be handled with regard to the child's capacity, best interests and applicable rights.

14.0 DATA BREACHES

A personal data breach includes accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. All suspected breaches must be reported internally without delay to the Data Protection Lead/DPO so that the school can contain the incident, assess risk, preserve evidence and record the outcome.

Where a breach is likely to result in a risk to individuals' rights and freedoms, the school will notify the ICO without undue delay and, where feasible, within 72 hours of becoming aware of it. Where a breach is likely to result in a high risk, affected individuals will also be informed without undue delay where required. The school will keep a record of personal data breaches, including those not reported to the ICO.

15.0 DATA PROTECTION COMPLAINTS AND CONCERNS

Individuals may raise concerns about how their personal data has been handled with the Data Protection Lead/DPO. The school will provide an accessible complaints route, acknowledge and investigate concerns, keep appropriate records and provide an outcome within a reasonable period. Individuals also have the right to raise concerns with the Information Commissioner's Office.

16.0 TRAINING, AUDIT AND COMPLIANCE MONITORING

Staff will receive data protection and information security training appropriate to their role, including induction and refresher training. The school will keep evidence of training and will periodically review records of processing, access controls, privacy notices, retention, contracts, data sharing, incidents and security measures to demonstrate ongoing compliance and improvement.

17.0 RECORDS AND DOCUMENTATION

The school will maintain appropriate accountability documentation, which may include records of processing activities, data maps/information asset registers, privacy notices, data sharing agreements, processor contracts, DPIAs, breach records, individual rights request logs, consent records where used, retention schedules and staff training records.

18.0 REVIEW OF THIS POLICY

This policy will be reviewed at least annually and sooner where there is a significant change in legislation, statutory or regulatory guidance, school systems, processing activities or identified risk. Changes will be approved through the school's normal governance arrangements and communicated to relevant staff.

RELATED GUIDANCE

- Department for Education: Data protection in schools (updated 9 July 2026).
- Information Commissioner's Office: UK GDPR guidance and resources, including subject access and personal data breach guidance.
- Everything Education School privacy notices, safeguarding policy, cyber security arrangements and retention schedule.