The American School in London

Data Protection Policy

Policy Owner (Accountable)	Director of Technology
Approved by	Buildings and Grounds Committee
To be ratified by B&G Committee on:	6 November 2026

1. Introduction

The American School in London Educational Trust Limited (data controller) maintains certain information (including personal and sensitive personal data) about its employees, students, parents, alumni and other community members, to allow it to communicate effectively with its community, to monitor employee and student achievement, and to ensure safety at the School. It is also necessary to process information so that employees can be recruited and paid; courses can be organized; a high standard of teaching and learning can be delivered, and legal obligations to funding bodies and government departments can be observed.

2. Purpose and Scope

This policy sets out how ASL handles personal information correctly and securely in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025 (DUAA), and other applicable legislation. It applies to information in any format, regardless of how it is collected, used, recorded, stored or destroyed, including paper and electronic records.

All employees, contractors, substitute teachers, athletics coaches, casual workers, temporary workers, trustees and volunteers who collect, use or disclose personal data must understand and comply with this policy.

3. Personal information

The American School in London (ASL) and individuals working on the School's behalf have access to a wide range of personal and sensitive data. The data may be held in a digital format or on paper records as part of a filing system. Personal data may be defined as any combination of data items that identifies a living individual and provides specific information about him/her, his/her family life, or personal circumstances. This includes:

- Personal information about members of the school community, including students, employees, parents or guardians, e.g., names, addresses, contact details, legal guardianship contact details, health records, disciplinary records, etc.
- Curricular or academic data, e.g., class lists, student progress records, reports, references
- Professional records, e.g., employment history, taxation and national insurance records, appraisal records and references
- Any data held visually in photographs or video clips (including CCTV) or as sound recordings
- Any expression of opinion about an individual kept on a school file or system, or any indication of the school's or someone else's intentions towards an individual
- Any other information that might be disclosed by parents or guardians, or by other agencies working with families or employees.

4. Data Protection Principles

ASL will comply with the seven data protection principles as follows:

1. ASL will process personal data lawfully, fairly and transparently by identifying and recording an appropriate lawful basis, providing clear privacy information and using personal data only in ways individuals would reasonably expect.
2. ASL will collect personal data for specified, explicit and legitimate purposes, record those purposes and assess compatibility before using the data for a new purpose.
3. ASL will collect, use and share only personal data that is adequate, relevant and limited to what is necessary for the stated purpose.
4. ASL will take reasonable steps to keep personal data accurate and up to date, provide routes for inaccuracies to be reported and correct or delete inaccurate data without undue delay.

5. ASL will retain identifiable personal data only for as long as necessary, in accordance with its approved retention schedule, and will securely delete, destroy or anonymise it when no longer required.
6. ASL will protect personal data against unauthorised or unlawful processing and accidental loss, destruction or damage through proportionate technical and organisational measures, access controls, staff training and incident-management procedures.
7. ASL will be responsible for, and able to demonstrate, compliance by assigning responsibilities, maintaining appropriate records, carrying out risk assessments and DPIAs where required, monitoring controls and reviewing compliance.

ASL employees and volunteers who process or use personal information must follow these principles at all times. A breach of this policy by an employee may result in disciplinary action.

ASL's privacy notices explain the lawful bases on which it processes personal data and special category personal data obtained from individuals or other sources. This policy does not form part of an employee's contract, although compliance with it is a condition of employment. ASL may amend the policy at any time.

5. Policy Statements and Responsibilities

The Board of Trustees has overall responsibility for ensuring that ASL complies with applicable data protection law.

The Director of Technology is responsible for overseeing this policy, coordinating compliance activities and reporting significant data protection risks or incidents to the Board.

<u>All Staff Responsibilities</u>

All staff are responsible for protecting personal data they access, process or handle in the course of their duties. Staff must comply with this policy and associated procedures, complete mandatory data protection training, maintain the confidentiality and security of personal data, and ensure that information is accessed, used, shared and retained only for authorised purposes. Any suspected or actual data breach, loss of personal data or data protection concern must be reported promptly in accordance with ASL's incident reporting procedures.

ASL will maintain appropriate records to demonstrate compliance.

ASL is committed to maintaining the data protection principles. It will:

- maintain its registration as a data controller with the Information Commissioner's Office (ICO);
- provide clear privacy information wherever personal data is collected;
- periodically check the quality and accuracy of information held;
- retain information only for as long as necessary, in accordance with an approved retention schedule;
- destroy obsolete information appropriately and securely;
- maintain proportionate safeguards against loss, theft and unauthorised disclosure, regardless of format;
- ensure employees and volunteers understand relevant policies and procedures;
- share personal information with third parties only where necessary and legally appropriate;
- maintain procedures for responding to requests for access to personal information, including subject access requests; and
- maintain appropriate records of processing activities.

Where information is subject to a common law duty of confidentiality, ASL must consider that duty separately from its obligations under data protection law. Confidential information may be shared with consent or where another lawful justification applies, including where sharing is necessary and proportionate to protect a child or another person from serious harm, meet a legal obligation or support another recognised public interest. Decisions to share without consent must be authorised by the Data Protection Officer, documented and limited to the minimum information necessary, unless an emergency requires immediate action.

ASL takes appropriate technical and organisational measures to protect personal data against loss, damage and unauthorised access.

6. Personal Data Breaches

A personal data breach includes the accidental or unlawful loss, destruction, alteration, unauthorised disclosure of, or access to, personal data. Examples include sending information to the wrong person, losing a device or paper file, inappropriate access, cyber incidents and failing to make personal data available when required.

Any actual or suspected breach must be reported immediately to the Data Protection Officer using ASL's personal data breach procedure. Individuals must take reasonable immediate steps to contain the incident, preserve relevant information and follow

instructions. They must not investigate independently, communicate externally or notify affected people unless authorised.

ASL will promptly investigate and record every reported breach, assess the risks to individuals and take appropriate remedial action. Where required, ASL will notify the Information Commissioner's Office without undue delay and, where feasible, within 72 hours of becoming aware of the breach. Where a breach is likely to result in a high risk to individuals, ASL will also inform affected individuals without undue delay.

7. Individual Information Rights

Individuals have rights over their personal data, including rights to be informed, access their personal data, correct inaccurate or incomplete information, request erasure or restriction, object to certain processing, receive certain data in a portable format, and obtain safeguards in relation to automated decision-making. These rights are not absolute and may be subject to legal conditions or exemptions.

Any individual covered by this policy who receives a request, whether made verbally or in writing, must forward it immediately to the Data Protection Officer and must not respond unless authorised. Staff must preserve relevant records and provide reasonable assistance with searches. ASL will verify identity where appropriate, record and assess each request, and respond within the applicable statutory timescale.

8. Data Protection Complaints

ASL will handle concerns and complaints about the use of personal data fairly, promptly and transparently. Complaints may be made by employees, students, parents or guardians, alumni or other individuals whose personal data ASL processes.

Any complaint received must be forwarded immediately to the Data Protection Officer. ASL will acknowledge, record and investigate the complaint, communicate the outcome and any corrective action, and explain the individual's right to raise the matter with the Information Commissioner's Office. Complaints will be used to identify recurring issues and improve practices.

9. Data Protection by Design and Default and DPIAs

ASL will consider data protection and privacy at the earliest stage of every new or materially changed project, system, service, process or technology involving personal data, and throughout its lifecycle. By default, ASL will collect and use only the personal

data necessary for the stated purpose, limit access to those who need it, apply appropriate retention settings and select proportionate security controls.

The responsible project or service owner must consult the Data Protection Officer before implementation. A data protection impact assessment must be completed before processing begins where the proposal is likely to result in a high risk to individuals, including certain uses of new technology, systematic monitoring, large-scale special category data or children's data, profiling or automated decision-making. Identified risks and actions must be documented, approved and monitored. Processing must not begin while an unmitigated high risk remains without any required consultation with the Information Commissioner's Office.

10. Data Sharing and Processors

ASL will share personal data internally or with external organisations only where there is a clear purpose, an appropriate lawful basis and, where relevant, a condition for processing special category or criminal offence data. Sharing must be necessary, proportionate, secure and limited to the minimum information required. Regular or higher-risk sharing arrangements must be documented and reviewed.

Before appointing a supplier to process personal data on ASL's behalf, ASL will carry out proportionate due diligence and put in place a written contract containing the required data protection terms. Processors must act only on ASL's documented instructions, maintain appropriate security, support ASL's compliance obligations, control sub-processors and return or securely delete personal data at the end of the service. Supplier performance and risks will be monitored throughout the arrangement.

11. International Transfers

Personal data must not be transferred, accessed or otherwise made available outside the UK unless the proposed arrangement has been reviewed and approved by the Data Protection Officer. This includes remote access from another country and the use of overseas suppliers, support teams, hosting or cloud services.

ASL will identify and document a lawful transfer mechanism, complete any required transfer risk assessment, and implement appropriate contractual, technical and organisational safeguards. Transfer arrangements will be recorded and reviewed when the service, destination, legal framework or risks materially change.

12. Retention and Secure Disposal

ASL will retain personal data only for as long as it is needed for the purpose for which it was collected, or to meet a legal, regulatory, safeguarding, operational or evidential requirement. Retention periods and their rationale will be documented in ASL's approved retention schedule and applied consistently to paper and electronic records, including copies held in local folders, email and other systems.

When personal data is no longer required, it must be securely deleted, destroyed or irreversibly anonymised using an approved method. Disposal may be suspended where records are required for an active complaint, investigation, legal claim, safeguarding matter or other authorised hold. Departments and system owners must support regular review and disposal activity.

13. Training, Monitoring and Review

All individuals covered by this policy must complete data protection and information security training appropriate to their role when they join ASL and at suitable intervals thereafter. Additional training or guidance will be provided where roles involve higher-risk processing or where incidents, legal changes or assurance work identify a need. Completion will be recorded and followed up.

Monitoring and Assurance

ASL will undertake proportionate monitoring and assurance activities to assess compliance with this policy and applicable data protection legislation. Significant findings, risks and areas for improvement will be reported to the appropriate senior leadership and the Data Protection Officer, with corrective actions identified and monitored as necessary.

This policy will be reviewed at least annually and sooner where there is a significant legal, organisational or technological change, a serious incident or a material control weakness. Supporting procedures, guidance and records must be kept consistent with the policy.

Privacy notices for parents, guardians and students will be made available through the School's website and other electronic communications. Parents or guardians of prospective students will receive the relevant privacy notice through the Admissions

Portal. Employees will have access to relevant privacy notices through ASL's internal platforms and communications.