The American School in London

Biometric Data Policy

The current version of any policy, procedure, protocol or guideline is the version held on the ASL website. It is the responsibility of all employees to ensure that they are following the most up-to-date version.

Responsible person	Director of Technology
Approved by	Director of Safeguarding and Compliance
Approval date	June 2025

Purpose and scope

This Policy sets out how the American School in London ("ASL", "we", "us") collects, uses, stores and deletes biometric data (currently fingerprint templates and face biometric data) for all students and staff who choose to enrol or whose data is processed under a lawful basis in the School's biometric system. At present biometric data is used to identify individuals for cash-free purchases and, in limited cases, to support safeguarding through facial recognition tagging (e.g., for school photos with parental permission or legitimate interest assessments) and to reduce queue times in the cafeteria. The same secure biometric platform may in future be extended to other authorised school services (for example secure printing, library circulation or attendance registration) without the need to recapture fingerprints. Any additional function will be covered by this Policy provided a fresh Data Protection Impact Assessment confirms compatibility.

Legal bases for processing

ASL relies on different lawful bases under the UK GDPR depending on the type of biometric data and its purpose:

- For fingerprint biometrics (e.g., used in the catering system), processing is based on:
    - **Legitimate interests** (UK GDPR Article 6(1)(f)): to provide an efficient, cash-free catering service.
    - **Explicit consent** (UK GDPR Article 9(2)(a)): required due to the sensitive nature of biometric data.

- For facial recognition (e.g., used in Pixevety for photo tagging and safeguarding purposes), processing is based on:
    - **Legitimate interests** (UK GDPR Article 6(1)(f)): to support safeguarding and community engagement.

    - **Substantial public interest** (UK GDPR Article 9(2)(g)), supported by appropriate policy safeguards.

ASL has conducted Data Protection Impact Assessments (DPIAs) and Legitimate Interests Assessments (LIAs) to assess and document these activities. The assessments concluded that the residual risks are low and proportionate, and that individuals' rights are upheld. Opt-out options are available to students, families, and employees for all facial recognition processing.

Consent and objection

Fingerprint biometrics (e.g., catering):

- Students require explicit consent from at least one parent or guardian, submitted electronically through the Veracross Family Portal (*Update Household Profile > Fingerprint Biometrics)* before enrolment in the system.

Facial recognition (e.g., Pixevety):

- Prior consent is not required, as processing is based on legitimate interests.
- However, families can object at any time through the Veracross Family Portal (*Update Household Profile > Photo Consent Form*)

Right to refuse: A student above the age of thirteen may also offer a verbal or written objection at any time.

Withdrawal of consent:

- Families may **withdraw consent** for their children at any time by updating the Biometrics Data Form in Veracross.
- Staff may choose not to enroll in fingerprint biometrics and can object to participating in facial recognition processing.

Consent validity: Consent remains valid for the duration of student enrolment or staff employment. ASL does not request annual re-confirmation but reminds individuals that changes can be made at any time.

Alternative arrangements

Use of biometrics is wholly optional. Individuals who do not enrol in fingerprint biometrics for catering or who later withdraw consent may obtain services by presenting their existing ASL photo ID card at the point of service.

Individuals who object to facial recognition biometrics will have their identification removed from Pixevety platform for photo tagging and will not have their photos published by ASL on any external platforms. Their photos may continue to appear on internal platforms that are secure and only accessible to the ASL community.

Data security and storage

When biometric data is collected (e.g., a fingerprint or facial image), a secure mathematical representation (called a template) is generated. For fingerprints, the original image is not stored and cannot be reconstructed from the template. This applies to systems like ASL's catering system provided by CRB Cunninghams.

For facial recognition, the official school portrait photo (stored in the Veracross school information system) is used to support recognition and tagging in platforms such as Pixevety. This image is processed securely and used only within ASL's safeguarded systems for approved purposes.

Biometric templates are stored in one of three places:

- On a secure server located on-premise in ASL's server room (e.g., for fingerprint data used in catering), or
- AWS cloud servers in the UK (e.g., for facial recognition processing by Pixevety)
- On school-issued devices (e.g., Touch ID / Face ID) if biometric authentication is enabled.

Fingerprint biometric data (used for catering) is stored locally on ASL's internal servers and never transmitted to cloud-based systems. Facial recognition data processed by Pixevety is securely handled via a cloud-based platform hosted on UK-based AWS servers under strict data processing agreements.

All communications between biometric devices (e.g., fingerprint readers) and servers are encrypted to protect data in transit.

Access control and administration:

- Access is strictly limited to authorised IT personnel and designated support staff.
- The vendors of biometrics systems (under contract) may access the database only as required and under data processing agreements and school direction.
- All administrative access is logged and reviewed regularly to ensure accountability.

Biometric use on school-issued devices:

- **School-issued student devices:** Biometric authentication (Touch ID or Face ID) is disabled by default. It can be enabled only with explicit parent or guardian consent submitted via the Veracross Parent Portal. Consent may be withdrawn at any time.
- **Staff devices:** Biometric authentication is also disabled by default but may be enabled voluntarily by staff. Doing so constitutes explicit consent, including agreement to the biometric provider's (e.g., Apple's) privacy policy.

Facial recognition (through Pixevety): Used to support safeguarding and photo consent through photo tagging in ASL's secure media platform. This processing is based on legitimate interests and is optional: parents may object to their children's images used for facial recognition at any time.

Biometric use on personal devices or for purposes outside defined ASL systems is not covered by this policy and is the responsibility of the individual user.

Retention and disposal

- Biometric data is kept for the duration of student enrolment or staff employment.
- Automatic deletion: Biometric data is deleted seven days after the withdrawal or leaving date as recorded in Veracross student information system. This includes deletion of both fingerprint templates and any face biometric data stored in school-controlled systems. Audit logs of the deletion are retained for 12 months.

Data sharing and third parties

Biometric data is disclosed only to the contracted biometric system providers solely for system maintenance under a data processing agreement. Templates are never shared with any other third party or used for any purpose beyond those listed above.

Individual rights

Individuals have the rights of access, rectification, erasure, restriction, objection and data portability as set out in the School Privacy Notices. Requests should be sent to dpo@asl.org. Complaints may be lodged with the UK Information Commissioner’s Office (ICO) via their main helpline on 0303 123 1113 .