



General Data Protection Policy and Statement

Glendale International School | Governance and compliance

Policy owner	Aarti Chauhan – Data Protection Lead,	Approval body	Jasmit Kang, Principal.
Effective date	2 September 2026	Review date	September 2027
Version	1.2	Policy number	GIS DP 01
Applies to	Staff, governors, contractors and learners where relevant	Status	Approved

Glendale International School is committed to keeping personal information safe, secure, accurate and used only for clear educational, safeguarding, employment, operational and legal purposes. As a school in Dubai, it applies applicable UAE data protection, education, safeguarding and employment requirements and maintains recognised data protection principles as school good practice.

Registration and contact details

Data Protection Officer or designated lead: Aarti.

Contact email and postal route: arti.chauhan@globalschools.com, Umm Al Hurair, Oud Metha (Next to American Hospital), Dubai, UAE.

1 Purpose and scope

This policy explains how the school handles personal data about learners, parents and carers, staff, applicants, alumni, volunteers, contractors, visitors and other individuals. It applies to paper and electronic records, photographs, audio and video, CCTV, emails, learning platforms, school systems, portable devices and information shared with trusted parties.

2 Legal and regulatory framework

- UAE Federal Decree-Law No. 45 of 2021 Regarding the Protection of Personal Data and its applicable executive requirements.
- Other applicable UAE education, safeguarding, employment, health, records, cybercrime and regulatory requirements.
- Recognised data protection principles adopted by the school as good practice.
- Contractual, assessment, certification and quality assurance requirements that apply to the school.

If two requirements differ, the school will obtain advice and follow the requirement that legally applies to the activity while maintaining the strongest lawful protection for individuals. This policy does not reduce any safeguarding duty or lawful requirement to disclose information to a competent authority.

3 Data protection principles

- Lawfulness, fairness and transparency: explain how and why information is used and rely on an appropriate legal basis.
- Purpose limitation: collect and use information only for specified legitimate purposes, unless further use is lawful and compatible.
- Data minimisation: collect only information that is adequate, relevant and necessary.
- Accuracy: take reasonable steps to keep information correct and current.
- Storage limitation: retain identifiable information only as long as needed.
- Integrity and confidentiality: protect information against loss, misuse, unauthorised access, disclosure, alteration or destruction.
- Accountability: document decisions and demonstrate compliance through policies, records, training, contracts, risk assessment and review.

4 Governance and responsibilities

Role	Responsibility
------	----------------

Principal	Accountable for school compliance, resources, governance, high-risk decisions and regulatory notification.
Data Protection Officer or designated Data Protection Lead	Advises the school, monitors compliance, supports impact assessments and rights requests, maintains relevant records and acts as the contact point for data concerns.
Assessment and Quality Leads	Ensure learner, assessment and quality assurance data is accurate, securely handled, shared only as required and retained appropriately.
IT and system owners	Apply access controls, secure configuration, backups, monitoring, disposal and supplier oversight.
All staff and authorised users	Follow this policy, use approved systems, keep information confidential, complete training and report incidents immediately.

Data protection contact: Data Protection Officer or designated Data Protection Lead, Glendale International School, Dubai. The school must publish the current contact email and postal route in its privacy notice and on the staff policy portal.

5 Personal data collected and purposes

Category	Examples and purposes
Learner and family records	Identity, contact, admissions, attendance, learning, behaviour, SEND, EAL, safeguarding, health, wellbeing, transport, finance and communication records used to educate, support and protect learners and operate the school.
Assessment records	Programme enrolment, evidence, assessment decisions, reasonable adjustments, internal quality assurance, appeals, certificates and related records.
Staff and workforce records	Recruitment, identity, vetting, qualifications, contracts, payroll, performance, attendance, health and professional development.
Site and technology records	Visitor logs, CCTV, access records, device and network logs used for security, safety, incident investigation and service operation.
Communications and media	Emails, consent choices, photographs, video and publications used for school communication, events and approved promotional purposes.

Special category or otherwise sensitive information, including health, disability, safeguarding, biometric, religious or ethnicity information, receives enhanced protection and is accessed only where necessary and lawful.

6 Lawful use transparency and consent

The school identifies and records an appropriate legal basis before processing. Depending on the activity, this may include legal obligation, public or educational functions, contract, protection of vital interests, legitimate interests assessed against individual rights, or consent. Sensitive information requires an additional lawful condition. Consent will be specific, informed, freely given where required, recorded and capable of withdrawal. Withdrawal does not make earlier lawful use invalid. Privacy notices will explain the controller, purposes, categories, legal basis, recipients, retention, transfers, rights and contact route in clear language suitable for the audience.

7 Collection accuracy and access

- Collect information directly where practicable and explain mandatory and optional fields.
- Verify identity and key records at appropriate points and provide routes for updates.
- Use role-based access and least privilege. Access is removed or changed promptly when roles change.
- Do not use personal email, unapproved cloud storage, personal messaging accounts or removable media for school personal data unless specifically authorised and protected.

- Check recipients and attachments before sending; use secure transfer, password protection or encryption where risk requires it.
- Keep paper records in secure storage and apply clear-desk, secure printing and confidential disposal arrangements.

8 Sharing processors and international transfers

Personal data may be shared with regulators, education authorities, safeguarding and health agencies, examination or assessment bodies, service providers and professional advisers only where there is a lawful and necessary purpose. The school will verify recipients, minimise the data shared, use secure methods and keep an appropriate record.

Suppliers processing personal data for the school must be subject to due diligence and written terms covering instructions, confidentiality, security, sub processors, assistance with rights and breaches, deletion or return, and audit. International transfers will use a lawful transfer mechanism and additional safeguards where required. The school will consider the destination, data sensitivity, access risks and protective measures before transfer.

9 Retention and secure disposal

The following is the school's minimum internal retention schedule. A longer period required by applicable UAE law, a regulator, safeguarding duty, contract, audit or legal hold takes priority. The detailed schedule identifies the record owner, purpose, legal or operational basis, retention trigger, period and disposal method. Where a safeguarding concern, complaint, appeal, investigation or audit is active, relevant records must not be destroyed until release is authorised.

Record type	Minimum policy position
Assessment, quality assurance, appeal and conflict records	Retain for at least three academic years after completion or closure, and longer where regulatory, safeguarding, contractual or legal requirements apply.
Complaints records	Retain for at least three academic years after closure, and longer where linked to safeguarding, litigation, an external review or a legal hold.
Safeguarding and child protection records	Retain and transfer in line with applicable safeguarding and education requirements; never apply routine deletion without safeguarding lead approval.
Core learner, academic and admissions records	Retain for enrolment plus three academic years after leaving, unless a longer education, safeguarding, certification or legal requirement applies.
HR and personnel records	Retain for employment plus two years, unless a longer statutory, pension, safeguarding, claims or legal requirement applies.
Finance and contract records	Retain for five years after the transaction or contract ends, unless a longer tax, audit, contractual or legal requirement applies.
CCTV recordings	Normally retain for 30 days; preserve relevant footage longer where required for an incident, safeguarding matter, investigation, claim or legal hold.
Visitor and access logs	Retain for one year, unless linked to an incident, safeguarding matter, investigation or legal hold.
Unsuccessful recruitment records	Retain for six months after the process closes, unless consent or a lawful requirement supports a longer period.

Expired records	Delete securely from active systems and backups in accordance with technical capability, or confidentially destroy paper and media, with evidence where appropriate.
-----------------	--

10 Individual rights and requests

Subject to applicable law, individuals may ask for access to their personal data, correction of inaccurate data, deletion, restriction, objection, data portability, information about processing, withdrawal of consent, or review of a significant solely automated decision. Rights are not absolute and may be limited by safeguarding, confidentiality, legal claims, another person's rights or other lawful exemptions.

1. Send a request to the Data Protection Officer or designated Data Protection Lead. No special wording is required. Staff who receive a request must forward it immediately.
2. Record the request and verify identity proportionately. Clarify scope where necessary without delaying unfairly.
3. Search all relevant systems and consult record owners. Review material for third-party information, safeguarding risk and lawful exemptions.
4. Respond without undue delay and within the timeframe required by the law or authority applicable to the request.
5. Keep a secure record of the request, searches, decision, disclosed material and response. Explain any refusal or limitation and the route for complaint.

11 Security and privacy by design

- Use multi-factor authentication where available, strong unique credentials, device encryption, supported software, patching, malware protection, backups and secure network controls.
- Review access rights periodically and monitor privileged and unusual access.
- Complete a data protection impact assessment before high-risk processing, such as systematic monitoring, new sensitive-data systems, biometrics or large-scale profiling.
- Build privacy requirements into new systems, projects, forms, apps and contracts from the start.
- Test restoration and incident response arrangements and securely erase or destroy retired devices and media.

12 Personal data breach procedure

1. Report any suspected loss, misdirection, unauthorised access, disclosure, alteration, destruction or unavailability immediately to the Data Protection Lead and IT. Do not wait for certainty and do not investigate privately.
2. Contain the incident: recover or recall information where safe, disable compromised access, preserve evidence, and protect affected individuals.
3. Log the facts, date and time discovered, data and people affected, likely consequences, containment and decisions.
4. Assess likelihood and severity of harm, including safeguarding, identity theft, discrimination, financial loss, confidentiality and distress.
5. The Principal and Data Protection Lead decide whether notification is required. Any applicable UAE authority, education regulator, police, safeguarding body, awarding organisation or insurer will be notified without avoidable delay and within the applicable legal or contractual timeframe.
6. Inform affected individuals without undue delay where the risk is high or where otherwise required, using clear advice on protective steps.
7. Complete root-cause analysis, corrective action and lessons learned. Record every breach and the rationale for notification or non-notification.

13 Assessment and learner data

- Use assessment information only for approved teaching, learning, registration, assessment, internal quality assurance, certification and review activities.
- Verify learner identity and data accuracy before registrations, submissions or certification claims.



- Share portfolios or evidence through approved secure channels and remove unnecessary personal or sensitive information.
- Limit access to authorised school staff and approved external personnel with a genuine need to know.
- Report any incident that may affect learner data, assessment integrity or certification promptly through the school's incident route and to any relevant external organisation when required.

14 Concerns complaints and escalation

Questions, rights requests or concerns should first be sent to the Data Protection Officer or designated Data Protection Lead. A person may use the school complaints procedure if dissatisfied. Nothing prevents an individual from contacting the competent data protection or education authority where they have that right. The school will not disadvantage anyone for raising a concern in good faith.

15 Training assurance and review

All staff will complete data protection and information security induction and periodic refresher training. Staff handling sensitive, safeguarding, HR, finance, IT or assessment data will receive role-specific guidance.

Compliance will be checked through access reviews, incident trends, supplier reviews, retention activity, sample audits and policy review. This policy is reviewed annually and sooner after legal change, a serious incident or new high-risk processing.

Appendix A Immediate breach reporting checklist

- What happened, when, and when was it discovered?
- Which systems, paper files, devices, emails or accounts are involved?
- What categories and approximate number of people and records are affected?
- Does the information include children, safeguarding, health, SEND, financial, identity or login data?
- Has the information been recovered, recalled, deleted by the wrong recipient or access disabled?
- Who may have received or accessed it? Is there evidence of misuse?
- What harm could occur and what immediate protection is needed?
- Who has been informed internally and externally, at what time, and why?

