

DATA PROTECTION, PRIVACY AND CONFIDENTIALITY POLICY

Policy Reviewed – March 2026

Date of Next Review – March 2027

1. Purpose

Apple International School is committed to protecting the personal information and privacy of students, parents and guardians, staff and other individuals connected with the School. This policy sets out how personal data is collected, used, stored, shared, protected and disposed of, and establishes expectations for confidentiality and responsible information handling.

The School will apply this policy in a manner consistent with applicable laws and regulatory requirements in the United Arab Emirates, including the UAE Personal Data Protection Law (Federal Decree-Law No. 45 of 2021), together with applicable education, child-protection and information-security requirements.

2. Scope

This policy applies to all personal data processed by or on behalf of the School, whether held electronically, on paper, in photographs, recordings or other formats.

- Students and prospective students.
- Parents, guardians and emergency contacts.
- Teachers, administrative staff, support staff and school leaders.
- Volunteers, visitors, contractors, consultants and service providers.
- Any third party processing information on behalf of the School.
- All school systems, devices, applications, databases, email accounts, learning platforms, paper records, CCTV and other information repositories.

Photographs, video and audio recordings for legitimate school, safeguarding, security, communication or educational purposes, subject to applicable requirements and permissions.

- Staff recruitment, employment, payroll, attendance, performance and professional records.
- IT account, device, access-control and security information.
- Information required by education authorities, examination bodies, regulators or other lawful authorities.

3. Definitions

- Personal Data: Information relating to an identified or identifiable individual.
- Processing: Any operation performed on personal data, including collection, recording, storage, use, disclosure, alteration, retrieval or deletion.
- Confidential Information: Information that is not intended for public disclosure and must only be accessed or shared for an authorised purpose.
- Data Subject: The individual to whom personal data relates.
- Data Breach: A security incident resulting in accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.
- Sensitive Personal Data: Information requiring additional protection because of its nature or potential impact on an individual, including certain health, biometric or other protected information.

4. Policy Principles

The School will manage personal data according to the following principles:

- Lawfulness, fairness and transparency: Data will be processed lawfully, fairly and transparently.
- Purpose limitation: Data will be collected and used for specified, legitimate school purposes.
- Data minimisation: Only data that is reasonably necessary for the stated purpose will be collected.
- Accuracy: Reasonable steps will be taken to keep information accurate and up to date.
- Storage limitation: Data will not be retained longer than necessary, subject to legal, regulatory and educational record requirements.
- Security and confidentiality: Appropriate technical and organisational safeguards will be used to prevent unauthorised access, loss, misuse or disclosure.
- Accountability: The School will maintain appropriate procedures, records, training and oversight to demonstrate responsible data handling.

5. Personal Data the School May Collect

- Student identity and contact details, admission and enrolment information.
- Parent/guardian and emergency-contact information.
- Attendance, assessment, examination and academic-progress records.
- Behaviour, safeguarding and pastoral records where required for student welfare and school duties.
- Relevant medical, dietary, accessibility and support information where necessary.
- Photographs, video and audio recordings for legitimate school, safeguarding, security, communication or educational purposes, subject to applicable requirements and permissions.
- Staff recruitment, employment, payroll, attendance, performance and professional records.
- IT account, device, access-control and security information.
- Information required by education authorities, examination bodies, regulators or other lawful authorities.

6. Collection and Use of Personal Data

The School will collect personal data through appropriate and lawful means. Information may be obtained directly from individuals, parents/guardians, authorised representatives, previous schools, education authorities, examination bodies, service providers or other lawful sources.

Personal data may be used to:

- ☐ Provide education, assessment, student support and pastoral care.
- ☐ Maintain attendance, safeguarding, health and emergency arrangements.
- ☐ Communicate with students, parents/guardians and staff.
- ☐ Meet legal, regulatory, examination and reporting obligations.
- ☐ Manage admissions, enrolment, staffing and school administration.
- ☐ Protect the safety and security of people and school property.
- ☐ Operate and support approved educational and information-technology systems.
- ☐ Monitor and improve educational and administrative services.

7. Consent and Lawful Processing

Where consent is required, the School will seek it in an appropriate and understandable manner and will keep suitable records. Consent will not be treated as the only possible basis for processing where another lawful basis applies. The School may process information when necessary for legitimate school functions, contractual or administrative purposes, legal obligations, safeguarding, public interest or other circumstances permitted by applicable law.

Where processing involves children, the School will give particular consideration to the child's best interests, applicable consent requirements and safeguarding obligations.

8. Privacy and Confidentiality

All staff and authorised persons must treat personal and confidential information with care. Access is provided on a need-to-know and role-appropriate basis.

- ☐ Do not discuss confidential student or staff information in public areas or with unauthorised people.
- ☐ Do not leave confidential documents, screens or devices unattended where they can be viewed by others.
- ☐ Do not send personal information to personal email accounts or unauthorised messaging platforms.
- ☐ Do not photograph, copy, download or disclose records unless authorised and necessary for school duties.
- ☐ Do not share passwords or individual user credentials.
- ☐ Use school-approved systems for storing and communicating confidential information whenever available.
- ☐ Confidentiality continues after an individual's employment, placement, contract or relationship with the School ends.

9. Student and Child Privacy

The School recognises that students require particular protection. Student information will only be shared with staff or third parties when there is an authorised educational, safeguarding, administrative, legal or other legitimate need. Information relating to safeguarding concerns will be handled confidentially, but confidentiality will not prevent disclosure to appropriate safeguarding or legal authorities where required to protect a child or comply with law.

The School will follow applicable UAE child-protection requirements and the principle that the best interests of the child guide safeguarding decisions.

10. Access Controls and Information Security

- User accounts will be assigned according to job or educational need.
- Access permissions will be reviewed and changed when roles change or access is no longer required.
- Strong passwords and, where available, multi-factor authentication should be used for school systems.
- Devices containing personal data should be protected by passwords, encryption or other appropriate security controls.
- Sensitive records should be stored in secure locations with controlled access.
- Staff must report lost devices, suspected phishing, malware, accidental disclosure or other security incidents promptly.
- Paper records should be secured when not in use and disposed of using secure methods.

11. Data Sharing and Disclosure

The School may share personal data with authorised third parties where necessary and lawful, including education authorities, examination boards, healthcare or safeguarding professionals, technology providers, transport or other contracted service providers, and competent government or law-enforcement authorities.

Before sharing information, the School will consider the purpose, necessity, recipient, security and applicable legal requirements. Where a service provider processes data on behalf of the School, appropriate contractual and security arrangements should be established.

12. Photographs, Video, CCTV and School Communications

The School may use photographs, video or recordings for legitimate educational, safeguarding, security, communication and school-event purposes. Where consent or another lawful basis is required, the School will apply the relevant requirements.

- CCTV will be used for safety, security and related legitimate purposes and access will be restricted.
- Parents and students are not allowed to access or view cctv footages.
- Images and recordings of students should not be shared through personal social-media accounts or unauthorised platforms.
- Staff should follow School procedures before publishing student images or identifying information on public-facing channels.

- CCTV will be used for safety, security and related legitimate purposes and access will be restricted.
- Parents and students are not allowed to access or view cctv footages.
- Images and recordings of students should not be shared through personal social-media accounts or unauthorised platforms.
- Staff should follow School procedures before publishing student images or identifying information on public-facing channels.
- Requests concerning removal or restriction of an image will be considered in accordance with applicable law and School procedures.

13. Data Retention and Secure Disposal

The School will maintain retention schedules appropriate to different categories of records. Records will be retained for as long as necessary for educational, operational, safeguarding, legal, regulatory, examination or archival purposes, and then securely deleted, destroyed or anonymised when no longer required.

- Electronic records should be securely deleted or disposed of using approved procedures.
- Paper records containing personal data should be securely shredded or otherwise destroyed.
- Records subject to an investigation, legal requirement or safeguarding matter must not be destroyed until authorised.

14. Data Subject Rights

Subject to applicable law and any lawful exemptions, individuals may have rights concerning their personal data, including rights to obtain information about processing, request access, request correction of inaccurate data, and request restriction or cessation of certain processing. Requests should be directed to the School's designated data-protection contact.

The School will respond to valid requests within the timeframes and procedures required by applicable law.

15. Data Breach and Incident Reporting

Any suspected or actual loss, unauthorised access, accidental disclosure, hacking incident, misdirected email, lost device or other personal-data incident must be reported immediately to the School's designated data-protection or IT/security contact.

1. Contain the incident where safe and authorised to do so.
2. Do not delete evidence or attempt to conceal the incident.
3. Record what happened, what information may be affected and who may be affected.
4. Escalate the incident to the appropriate School leadership and relevant specialists.
5. Assess notification obligations and take any required corrective or protective action.

16. Responsibilities

School Leadership

- ☐ Approve and support this policy and ensure appropriate resources are available.
- ☐ Promote a culture of privacy, confidentiality and responsible information use.
- ☐ Ensure significant incidents and risks are appropriately managed.

Data Protection / Privacy Lead or Designated Contact

- ☐ Provide guidance on data protection and confidentiality.
- ☐ Coordinate data-subject requests and privacy-related enquiries.
- ☐ Support data-breach assessment, record keeping and regulatory communications where required.
- ☐ Coordinate policy review and staff awareness.

IT and System Administrators

- ☐ Implement appropriate technical safeguards and access controls.
- ☐ Maintain system security, backups and access management.
- ☐ Support incident investigation and remediation.

All Staff and Other Authorised Users

- ☐ Follow this policy and related School procedures.
- ☐ Only access information required for their role.
- ☐ Maintain confidentiality and complete required training.
- ☐ Report suspected data breaches or inappropriate access immediately.

Parents, Guardians and Students

- ☐ Provide accurate information and notify the School of relevant changes.
- ☐ Respect the privacy of other students, families and staff.
- ☐ Use School systems and information responsibly.

17. Training and Awareness

Relevant staff will receive appropriate data-protection, confidentiality, cybersecurity and safeguarding awareness. Training should be refreshed periodically and when significant changes to law, systems or School procedures occur.

18. Breaches of this Policy

Failure to comply with this policy may result in investigation and appropriate action under the School's staff, student, safeguarding, disciplinary or contractual procedures. Serious incidents may also be reported to competent authorities where required by law.

19. Policy Monitoring and Review

This policy will be reviewed at least annually and sooner where there are significant changes in law, regulatory requirements, school systems, risks or operating practices. The School will monitor implementation and update procedures where improvements are identified.

20. Related Documents

- ☐ School Safeguarding / Child Protection Policy.
- ☐ Acceptable Use and IT Security Policy.
- ☐ Records Retention and Disposal Procedure.
- ☐ Staff Code of Conduct.
- ☐ CCTV Policy / Procedure, where applicable.
- ☐ Complaints and Data-Subject Request Procedure.
- ☐ Relevant UAE data-protection, education and child-protection legislation and regulatory guidance.

Regards,

Kale

Principal

The Indian Academy,

Prarthana Kale

Principal Code: 90031