EBIS

EGYPT BRITANNIA INTERNATIONAL SCHOOL

NEW CAPITAL

DATA PROTECTION POLICY

Privacy • Security • Accountable

PROTECT	TRANSPARENT	SAFEGUARD	ACCOUNTABLE
Keep personal data secure	Use data fairly and openly	Prioritise children and sensitive data	Record decisions and responsibilities

GOVERNANCE & COMPLIANCE

EBIS protects the privacy, dignity and rights of its pupils, families, staff and wider community through lawful, secure and responsible data practice.

POLICY OWNER	Principal / Data Protection Officer
APPROVED BY	Board / Proprietor
EFFECTIVE FROM	September 2026
NEXT REVIEW	September 2027
POLICY STATUS	Active
SCHOOL	EBIS – New Capital

RELATED POLICIES

- Safeguarding and Child Protection Policy
- Admissions Policy
- Inclusion Policy
- Behaviour Policy
- Staff Code of Conduct
- BYOD / Acceptable Use of Technology Policy
- Complaints Policy

1. MISSION STATEMENT AND PURPOSE

Egypt Britannia International School (EBIS) is committed to protecting the privacy, dignity and rights of all members of its community. Lawful, fair and transparent handling of personal data is essential to safeguarding children, maintaining trust with families and staff, and ensuring responsible governance.

This policy ensures that personal and disclosure information is handled securely and proportionately, with safeguarding, wellbeing and accountability at the centre of decision-making.

2. POLICY STATEMENT

EBIS collects, processes, stores, shares and disposes of personal data in accordance with applicable Egyptian law. The school also draws on UK data-protection principles as a benchmark for good international practice where these are compatible with host-country law.

- Egyptian Personal Data Protection Law No. 151 of 2020.
- Executive Regulations issued under Ministerial Decree No. 816 of 2025.
- Relevant Egyptian education, employment, safeguarding, cybercrime and record-keeping requirements.
- UK GDPR and the Data Protection Act 2018 as international reference points for British-school good practice, rather than as the primary governing law in Egypt.

CURRENT EGYPTIAN FRAMEWORK

The 2025 Executive Regulations make Egypt's Personal Data Protection Law operational and introduce detailed requirements for controllers, processors, Data Protection Officers, children's data, breach reporting and cross-border transfers.

3. SCOPE

This policy applies to personal and disclosure information relating to:

- Students
- Staff, including academic, administrative, maintenance, temporary and supply staff
- Parents and guardians
- Contractors and service providers
- Visitors who may handle or be exposed to personal data

It applies to paper records, digital systems, CCTV, photographs and video, school devices, communications, cloud services and third-party platforms.

4. ROLES AND RESPONSIBILITIES

Board / Proprietor

Provides strategic oversight, approves the policy and review cycle, and assures itself that significant data-protection risks are managed.

Principal and Senior Leadership Team

Ensure whole-school compliance, appropriate resourcing, staff accountability and prompt action on significant risks or breaches.

Data Protection Officer (DPO)

Advises on lawful processing and risk management; monitors compliance; coordinates data-subject requests and breach management; maintains appropriate records and liaison with the competent Egyptian authority where required.

All Staff

Handle personal data securely and confidentially; access only what they need; follow school procedures; report suspected breaches immediately.

IT Department

Maintains secure systems, role-based access, backups, monitoring, patching and appropriate technical safeguards.

Third-Party Processors

Process data only for authorised purposes and under appropriate written contractual and security arrangements.

5. KEY PRINCIPLES

- **Lawfulness, fairness and transparency**
- **Purpose limitation**
- **Data minimisation**
- **Accuracy and currency**
- **Storage limitation**
- **Integrity and confidentiality**
- **Accountability and documentation**

6. DATA PROCESSING AND DISCLOSURE PROCEDURES

Lawful and Permitted Processing

EBIS identifies and documents an appropriate lawful ground or permission for processing personal data under applicable Egyptian law. Where consent is relied upon, it must be obtained and managed in accordance with the requirements applying to the relevant data and purpose.

Children's data and other sensitive personal data receive enhanced protection. The school will obtain parent or guardian involvement or consent where required by law and will apply additional security and access controls.

Use and Sharing of Information

Personal information is shared only where lawful, necessary, proportionate and consistent with the purpose for which it is held. This may include appropriate sharing with:

- Safeguarding, health, emergency or law-enforcement authorities where appropriate
- Recruitment and employment verification services
- Examination boards, universities and inspection/accreditation bodies
- Transport, security, payment, communications, MIS, cloud and IT service providers operating under appropriate contracts

Personal data is never sold. It will not be reused for an unrelated purpose without a valid legal basis and any additional notice or consent required.

7. STORAGE, SECURITY AND ACCESS CONTROLS

Physical Security

- Locked storage for confidential paper files
- Restricted access to sensitive records
- Secure shredding or approved confidential disposal

Digital Security

- Password-protected and role-based access
- Encryption and secure servers/cloud services where appropriate
- Firewalls, anti-malware, patching, backups and system monitoring
- Multi-factor authentication for higher-risk systems where available

CCTV

- Used for legitimate safeguarding, security and operational purposes
- Access restricted to authorised personnel
- Footage retained only for defined periods unless required for an incident or investigation

8. DATA RETENTION AND DISPOSAL

EBIS retains personal data only for as long as it is required for the purpose for which it was collected and to meet applicable legal, safeguarding, employment, financial and regulatory obligations.

RETENTION SCHEDULE

The school will maintain a documented retention schedule by record type. Fixed periods will be reviewed against current Egyptian legal requirements and the school's safeguarding and operational needs rather than copied automatically from another jurisdiction.

Secure disposal includes confidential shredding, secure digital deletion or wiping, and appropriate destruction or sanitisation of storage devices.

9. RIGHTS OF DATA SUBJECTS

Individuals may exercise the rights available to them under applicable Egyptian data-protection law. Depending on the circumstances, these may include rights relating to access, correction, erasure, withdrawal of consent, restriction or objection, and information about how their data is processed.

Requests should be directed to the DPO. The school will verify identity, record the request and respond within the timeframe required by applicable law and the Executive Regulations.

CHILDREN AND FAMILIES
Requests involving a child will be handled with particular care, taking account of the child's age, capacity, safeguarding needs and the legal rights of parents or guardians.

10. DATA BREACHES AND RISK MANAGEMENT

A personal data breach includes accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

1 RECOGNISE	2 REPORT	3 CONTAIN	4 ASSESS	5 NOTIFY
Identify loss, disclosure or unauthorised access	Tell the DPO immediately	Limit further exposure or loss	Record impact, risk and actions	Notify the competent authority / individuals where legally required

The DPO will coordinate containment, investigation, risk assessment, documentation and any notification required under Egyptian law. Where a breach may affect safeguarding, the DSL will be involved immediately.

11. THIRD PARTIES, CLOUD SERVICES AND CROSS-BORDER TRANSFERS

Before appointing a processor or digital service provider, EBIS will consider data security, confidentiality, access controls, location of data, sub-processors, breach arrangements, deletion/return of data and contractual safeguards.

Cross-border transfers of personal data will take place only where permitted by Egyptian law and the Executive Regulations and where any required approvals, licences, permits, contractual safeguards or consents have been obtained.

NEW SCHOOL SYSTEMS
Procurement of MIS, learning platforms, cloud storage, communications, payment, transport and security systems must include data-protection due diligence before personal data is transferred to the provider.

12. CHILDREN'S DATA, IMAGES AND SCHOOL COMMUNICATIONS

Children's personal data requires enhanced protection. EBIS will ensure that collection is limited to what is necessary, privacy information is understandable, access is restricted and parent/guardian involvement is obtained where legally required.

- Photographs and video used for school communications and marketing will be managed through clear school permissions and notices.
- Sensitive safeguarding, health, SEND and pastoral information will have restricted access.
- Staff must not use personal accounts, unapproved apps or unauthorised devices to store or share confidential pupil information.
- School communications must avoid unnecessary disclosure of personal information to groups or third parties.

13. TRAINING, MONITORING AND EVALUATION

- Data protection included in induction for all staff
- Regular refresher training for all staff
- Enhanced role-specific training for HR, safeguarding, IT, admissions and senior leaders
- Periodic review of access permissions, high-risk processing and third-party arrangements
- Recording and review of breaches, near misses and lessons learned

STAFF EXPECTATION
Every member of staff is responsible for protecting the personal information they access. Convenience is never a sufficient reason to bypass approved systems or security controls.

14. COMMUNICATION AND ACCESSIBILITY

This policy will be available to staff and families and supported by appropriate privacy notices. Relevant information will be communicated in clear language and, where appropriate, in formats accessible to pupils and parents.

15. POLICY REVIEW

This policy is reviewed at least annually by the Principal and DPO and approved by the Board / Proprietor. It will also be reviewed when Egyptian law or regulations change, when new systems or high-risk processing are introduced, or when a significant data incident identifies a need for revision.

OUR COMMITMENT
At EBIS, responsible data practice supports trust, safeguarding and effective education. We protect information because the people behind the data matter.