

6. Data Protection and Privacy

This section is designed to align with Qatar's Personal Data Privacy Protection Law (Law No. 13 of 2016, "PDPPL") and guidance issued by the National Cyber Security Agency (NCSA).

6.1 Types of Information

- Student identification, contact, academic, attendance, behaviour, medical, safeguarding and SEN information
- Parent and guardian contact details, communications and account credentials
- Staff HR, payroll, performance, attendance, medical and professional records
- Financial, procurement, legal, examination, assessment and operational records
- Security logs, CCTV footage, access records and cybersecurity information

6.2 Data Protection Principles

- Purpose limitation — information is collected and used only for legitimate school purposes
- Data minimisation — only information necessary for the purpose should be collected or shared
- Accuracy — reasonable steps should be taken to keep records accurate and up to date
- Access control — information is accessible only to authorised users with a legitimate need
- Secure storage — school information must be stored on approved systems
- Controlled sharing — information must be shared only with authorised recipients and through approved methods
- Retention — records are kept only as long as required by law, regulation, operational need or the approved retention schedule
- Secure disposal — information must be deleted, wiped or destroyed securely when no longer required
- Accountability — significant access, sharing, retention and incidents should be documented where appropriate

6.3 Data Classification

Information is classified into four tiers, each with its own handling rules:

Classification	Examples	Handling
Public	Published website content, public notices	May be shared publicly when authorised
Internal	Routine internal procedures, general staff communications	School use; share externally only where appropriate

"Empower students to learn for life and strive for excellence so that they can contribute positively to the global society"

Confidential	Student records, HR records, finance, assessments	Restricted to authorised users and approved systems
Highly Confidential / Restricted	Safeguarding, medical, legal, passwords, security configurations, sensitive investigations	Strict need-to-know access; enhanced security and controlled sharing

6.4 Approved Storage

Approved for school data:

- School-provided Microsoft 365 services, including OneDrive, SharePoint and Teams, where approved
- Approved school ERP and learning platforms
- Approved school network storage and managed school devices
- Other platforms expressly authorised through the school's digital-platform approval process (see section 17)

Not approved for confidential school data unless formally authorised:

- Personal email accounts
- Personal cloud storage such as personal Google Drive, Dropbox or iCloud
- Unencrypted or unauthorised USB devices
- Personal messaging applications such as WhatsApp where confidential school data would be transmitted
- Public AI tools

6.5 Data on Personal Devices

Confidential school information must not ordinarily be downloaded, stored or retained on personal devices. Where exceptional use is authorised, the minimum necessary data must be protected and removed promptly when no longer required.

6.6 Retention and Secure Disposal

The school will maintain an approved records-retention schedule (see Appendix L). Indefinite retention will be exceptional and must be justified by legal, regulatory or operational requirements. Backup copies do not replace the retention schedule and should not be used to retain records indefinitely.

Devices and storage media must be securely wiped before disposal, reassignment or external repair where appropriate.

“Empower students to learn for life and strive for excellence so that they can contribute positively to the global society”

6.7 Special Category (Sensitive) Data

Some information the school holds falls into a special, more sensitive category under the PDPPL, including:

- Health and medical information (e.g. allergies, chronic conditions, nurse records)
- Biometric data (e.g. fingerprint attendance records)
- Safeguarding, disciplinary, and behavioural records
- Religious or nationality information collected for curriculum or MoEHE reporting purposes

This information must be accessible only to staff who need it for their role, stored separately from general student records where practical, never shared over unencrypted channels, and reviewed by the Data Privacy Lead before being used for any new purpose beyond the one it was originally collected for.

6.8 Cross-Border Data Transfers & Cloud Hosting

Where possible, the school should use cloud services with data centres located in Qatar or otherwise offering equivalent safeguards, since transferring personal data outside Qatar carries additional obligations under the PDPPL. The IT Department should confirm the hosting location of any new cloud-based system before adoption, and where data must be hosted outside Qatar, confirm the provider offers appropriate contractual and security safeguards.