

DATA PROTECTION, PRIVACY & NETWORK SECURITY POLICY

GSPC British School

9, rue Abdeslame Amir, quartier Plateau Extension (Riviera), Casablanca, Morocco

Policy owner	Principals / Owner & CEO	Applies to	EYFS, Primary & Secondary; staff, pupils, families and contractors
Established	August 2026	Next review	July 2027
Status	Whole-school controlled policy	Version	1.0
Approval	Principals and Owner & CEO	Framework	Moroccan Law 09-08 / British educational standards

CORE PRINCIPLE Personal data must be lawful, necessary, accurate, secure and accessible only to authorised people. Network security, filtering and monitoring are part of protecting both data and pupils.

Contents

1. Purpose and legal context
2. Data protection principles
3. School systems and access
4. Network security, firewall, filtering and monitoring
5. Suppliers, contracts and cloud services
6. Images, communications, devices and AI
7. Data sharing, international transfers and safeguarding
8. Rights, requests, breaches and retention
9. Responsibilities, review and related policies

1. Purpose and legal context

GSPC British School processes personal information for legitimate educational, safeguarding, admissions, employment, health, operational and legal purposes. As a school operating in Morocco, the governing legal framework is Moroccan Law No. 09-08 and the requirements of the Commission Nationale de contrôle de la protection des Données à caractère Personnel (CNDP). British school data-protection and cyber-security guidance is used as a professional benchmark where compatible with Moroccan law. UK GDPR and UK data-protection legislation are not presented as directly binding Moroccan law. Where systems, suppliers or services involve data outside Morocco, the school checks the applicable CNDP requirements before transfer or hosting.

2. Data protection principles

- Collect and use only information that is necessary, relevant and connected to a clear school purpose.
- Keep data accurate and update it when necessary.
- Limit access according to role and need-to-know; sensitive information receives additional protection.
- Use appropriate technical and organisational security to protect against loss, alteration, unauthorised disclosure or access.
- Keep records only for as long as required by legal, safeguarding, educational or operational needs, then dispose of them securely.
- Tell people, through appropriate notices and communications, how their information is used and protected.
- Report suspected loss, cyber incident, unauthorised access or disclosure immediately.

3. School systems and access

G-EcolePlus is the approved shared operational system for attendance, lesson logs, homework, digital resources, assessment/data, admissions information and parent communication. Safeguarding concerns are currently recorded through the separate approved safeguarding process and secure restricted records; safeguarding functionality must not be moved into G-EcolePlus without an approved implementation and access-control review.

- Staff use individual authorised accounts and must not share passwords or leave systems accessible to unauthorised users.
- Access permissions should reflect the user's role and be reviewed when staff join, change role or leave.
- Sensitive SEND, medical, HR and safeguarding information is restricted to staff who require it for their role.
- School information must not be copied to unauthorised personal email, cloud storage, messaging or social-media accounts.

4. Network security, firewall, filtering and monitoring

GSPC maintains a professionally installed and contracted firewall/filtering solution to protect the school network and support safe internet use. The solution forms part of the school's technical and organisational security controls and should be configured, supported and reviewed in line with the school's risk profile.

- The firewall should protect the network against unauthorised access and known malicious traffic, with security updates and configuration maintained through the contracted support arrangement.
- Filtering should block illegal, harmful and inappropriate content without unnecessarily preventing legitimate teaching, learning or administration.
- Monitoring may include network logs, web-access records, alerts and appropriate staff supervision. Access to monitoring information is restricted to authorised personnel.
- High-risk technical or safeguarding alerts should be escalated promptly; routine reports/logs should be reviewed at an agreed frequency and significant actions recorded.
- Filtering and monitoring must cover school-managed devices and the school network; BYOD and guest access must be considered within the configuration and risk assessment.
- The school should review filtering and monitoring at least annually and following a significant incident, material network change or change of provider. No system is treated as 100% effective, so staff supervision, online-safety education and incident reporting remain essential.

FIREWALL EVIDENCE TO RETAIN Current supplier/service contract; installation/configuration record; support and renewal details; named school contact; filtering categories/rules; monitoring/reporting arrangements; review records; incident/escalation route; evidence of updates and significant configuration changes.

5. Suppliers, contracts and cloud services

Where a supplier processes personal data for GSPC, the school must select providers offering appropriate security and confidentiality guarantees and ensure these obligations are reflected in the contractual arrangement. This applies to G-EcolePlus, cloud services, filtering/firewall support and other EdTech or IT providers.

- Before introducing a significant new system, the school reviews what data is collected, where it is hosted, who can access it, security controls, retention/deletion, incident notification and any overseas transfer.
- Contracts should identify the service, responsibilities, confidentiality/security expectations, support arrangements and what happens to school data at contract end.

- Where appropriate, the school may require supplier evidence of security controls, audit/assurance information or remedial action.
- CNDP notification, prior authorisation or overseas-transfer formalities are completed where required by Law 09-08 before the relevant processing/transfer is implemented.

6. Images, communications, devices and AI

- Staff use approved school communication channels and follow the Staff Code of Conduct, Online Safety/ICT and BYOD policies.
- Pupil images and recordings are used only for legitimate school purposes with the appropriate school/parental permissions and safeguards.
- Personal information and pupil records must not be stored or shared through unauthorised personal accounts, WhatsApp/social media or personal cloud storage.
- Confidential pupil, family, staff, medical, SEND or safeguarding information must not be entered into an unapproved generative-AI tool. Staff remain responsible for checking AI outputs and protecting personal information.
- Personal devices may only access school information where authorised and appropriately secured; loss or compromise must be reported immediately.

7. Data sharing, international transfers and safeguarding

Personal data is shared only where there is a legitimate, lawful and necessary reason. Safeguarding information may be shared on a need-to-know basis where necessary to protect a child, following the Safeguarding & Child Protection Policy and applicable Moroccan requirements.

Where personal data will be hosted or transferred outside Morocco, the school checks the destination, purpose, contractual safeguards and applicable CNDP transfer requirements before implementation. Cloud use is not treated as automatically exempt from overseas-transfer requirements.

8. Rights, requests, breaches and retention

- Requests concerning personal data, correction, access or objection are referred promptly to the relevant Principal/SLT for handling under Moroccan law and CNDP requirements.
- Any suspected data breach, lost device, misdirected email, unauthorised disclosure, compromised account, malware or cyber incident must be reported immediately to leadership/IT support.
- The school contains the incident, preserves relevant evidence, assesses risk, documents decisions and contacts affected persons and/or the competent Moroccan authority where legally required.
- Retention periods are based on the purpose of the record, safeguarding needs, applicable Moroccan requirements and legitimate school needs. Secure deletion or destruction is used when retention is no longer justified.

9. Responsibilities, review and related policies

- Owner & CEO / Principals: accountability, resources, contracts, significant decisions and escalation.
- SLT / administration / IT support: access controls, systems, supplier coordination, security reviews, incident response and staff implementation.
- DSL/DDSL: safeguarding information-sharing decisions and safeguarding implications of online incidents.
- All staff: secure handling, approved systems, confidentiality, password/account security and immediate reporting of concerns.

The policy is reviewed annually and sooner following a significant data/cyber incident, material system or supplier change, or change in applicable Moroccan requirements.

Related policies: Safeguarding & Child Protection; Online Safety, ICT & Acceptable Use; BYOD; Staff Code of Conduct; Admissions; SEND; First Aid / Medical; Complaints; Records/retention procedures; contractual IT and firewall/filtering arrangements.

Document control and current leadership

Ratified	Next review	Principal - Secondary	Principal - Primary & EYFS	Owner & CEO
6 July 2026	July 2027	Hannah Cashel	Jihane El Antri	Hicham Lazrak