

ONLINE SAFETY DIGITAL SECURITY AND ACCEPTABLE USE POLICY

Document Control	Details
School	Richmond International School Doha
Policy Owner	Executive Principal
Operational leads	IT Manager/Data Protection Lead
Oversight	Board of Directors
Review date	August 2027, or earlier following a serious incident, material system change or new official requirement
Applies to	Pupils, employees, volunteers, visitors, contractors, parents and carers using or interacting with school digital services
Related documents	Safeguarding and Child Protection Policy; Data Protection Policy; Staff Code of Conduct; Behaviour Policy; Anti-Bullying Policy; Social Media Policy; Photography and Media Consent procedures; Crisis and Emergency Management Plan



Online Safety Digital Security and Acceptable Use Policy

Contents

1 Purpose and policy principles	3
2 Scope.....	3
3 Regulatory and professional framework	4
4 Definitions and online risk categories	5
5 Roles and responsibilities	6
6 Acceptable and responsible use.....	7
6.1 General requirements.....	7
6.2 Prohibited activity.....	7
7 Accounts passwords and access permissions	8
8 Network security filtering and monitoring	8
8.1 Technical protection	8
8.2 Filtering	8
8.3 Monitoring	9
9 Personal data privacy and records.....	9
10 School devices personal devices and removable media.....	10
10.1 School devices	10
10.2 Personal devices and bring your own device arrangements.....	10
10.3 Removable media and charging.....	10
11 Communication email and social media.....	11
12 Images video audio and live streaming	11
13 Online safety education and training	12
13.1 Pupil education	12
13.2 Staff training.....	12
13.3 Parent awareness	12
14 Reporting safeguarding and incident response	12
14.1 How to report	12
14.2 Immediate response.....	13
15 Cyberbullying and online conduct outside school.....	13
16 Harmful content grooming and sexual imagery	13



RICHMOND INTERNATIONAL SCHOOL

مدرسة ريتشموند الدولية

17 Artificial intelligence	14
18 Remote learning video conferencing and recordings	14
19 Third party systems and cloud services	15
20 Cyber incidents personal data breaches and continuity.....	15
20.1 Examples.....	15
20.2 Response.....	15
20.3 Business continuity	16
21 Investigation sanctions and restoration	16
22 Monitoring assurance and evidence	17
23 Complaints review and approval	18
Appendix A Staff acceptable use agreement.....	19
Appendix Key Stage 1 Pupil agreement	20
Appendix C Key Stage 2 pupil acceptable use agreement.....	21
Appendix D Online safety incident response card	22
Appendix E Cyber incident and data breach checklist	23
Appendix F Termly compliance audit and evidence schedule	24
Reference sources.....	25



1 Purpose and policy principles

Richmond International School recognises that technology is essential to teaching, learning, assessment, communication and school leadership. Digital access also creates risks to children, employees, information and school operations. This policy defines the controls that RIS will use to reduce those risks, respond consistently to concerns and teach pupils to become safe and responsible digital citizens.

RIS will apply the following principles:

- **Safeguarding first.** Online concerns are treated as safeguarding matters whenever a child may be at risk of harm.
- **Age-appropriate access.** Access, supervision, curriculum content and controls reflect pupils' ages, maturity and individual needs.
- **Security by design.** Access is limited to what each role requires, systems are configured securely and personal data is protected throughout its lifecycle.
- **Transparency and proportionality.** Filtering and monitoring are explained, authorised and proportionate to safeguarding and security risks.
- **Education as well as control.** Technical controls are supported by curriculum teaching, staff training and parent awareness.
- **Prompt reporting.** Pupils and adults can report concerns without fear of blame, and serious matters are escalated immediately.
- **Evidence and improvement.** Checks, incidents, decisions and actions are recorded and reviewed so that practice improves over time.

2 Scope

This policy applies whenever a person accesses or uses:

- School networks, internet connections, devices, accounts, email, websites, management systems and cloud services.
- School-approved learning and communication platforms, including ClassDojo, Microsoft 365, Teams and any subsequently approved system.
- Personal devices connected to a school network or used for school work, communication or school-related content.
- Digital content created, stored, shared or published on behalf of RIS.
- Online activity outside school where it creates a safeguarding, bullying, confidentiality, data-security, reputational or operational concern for a pupil, employee or the school community.

The policy applies to pupils, employees, volunteers, contractors, visitors, parents and carers. It covers the school day, clubs, educational visits, remote learning, transport where school systems are used and any school-organised activity.



3 Regulatory and professional framework

RIS will apply this policy alongside current Qatar requirements and official instructions. Relevant sources include:

- Ministry of Education and Higher Education requirements and the Guidelines for the Mandatory Evaluation Process for Private Schools 2026, including expectations for clear digital-security procedures, technical protection, role-based access and regular awareness programmes.
- Qatar Law No. 13 of 2016 on Protecting Personal Data Privacy and guidance issued by the National Cyber Security Agency.
- Qatar Law No. 14 of 2014 on Cybercrime Prevention, where applicable.
- Current official safeguarding, child-protection, communications and cybersecurity instructions issued by competent Qatar authorities.
- Keeping Children Safe in Education 2026 as a non-statutory international safeguarding benchmark for RIS.

If any part of this policy conflicts with a current Qatar legal or official requirement, the Qatar requirement prevails. The Executive Principal will arrange prompt amendment of the policy and associated procedures.



4 Definitions and online risk categories

Term	Meaning in this policy
Online safety	Safeguarding people from harm arising through internet-connected technology, digital communication, content or services.
Digital security	Protecting systems, networks, accounts, devices and information from unauthorised access, loss, alteration, disruption or misuse.
Personal data	Information relating to an identified or identifiable person, including pupil, parent, employee, health, assessment, safeguarding, image and identification data.
Data breach	Accidental or unlawful loss, disclosure, access, alteration, destruction or unavailability of personal data.
School-approved platform	A service formally authorised by RIS following safeguarding, privacy, security and educational review.
Monitoring	Authorised review of network, account or device activity for safeguarding, security, compliance and operational purposes.

RIS uses the following four categories to structure online risk assessment and teaching:

Risk category	Examples
Content	Violent, sexual, discriminatory, extremist, self-harm, suicide, misinformation, age-inappropriate or otherwise harmful material.
Contact	Grooming, coercion, unwanted contact, impersonation, requests for images, sextortion, exploitation or contact from unknown adults or peers.
Conduct	Cyberbullying, harassment, sharing private information, harmful challenges, non-consensual recording, plagiarism, hacking or creating harmful content.
Commercial and contractual	Scams, phishing, gambling, in-app purchases, advertising, data exploitation, unfair terms and unauthorised subscriptions.



5 Roles and responsibilities

Role	Responsibilities
Board of Directors	Approve the policy; ensure sufficient resources and appropriate oversight; receive termly assurance and reports on serious incidents; challenge gaps and monitor completion of actions.
Executive Principal	Overall accountability; ensure Qatar requirements are followed; appoint competent leads; approve systems and significant monitoring; coordinate serious incidents and external reporting; ensure actions are completed.
Designated Safeguarding Lead	Lead safeguarding assessment and response; maintain safeguarding records; advise on pupil risk; coordinate parent and authority contact; review safeguarding alerts and online-safety education.
IT Manager/ Data Protection Lead	Maintain secure infrastructure, filtering, monitoring, backups, patching, anti-malware, device and account controls; keep technical logs and inventories; contain cyber incidents; report risks to SLT. Advise on privacy compliance; maintain data-processing and breach records; review privacy notices, retention and third-party processing; coordinate required data-breach assessment and notification.
SLT and MLT	Implement expectations in their areas; monitor supervision and curriculum delivery; ensure staff report concerns; support incident review and corrective actions.
Teachers and support staff	Supervise age-appropriately; use approved systems; teach and model safe behaviour; protect credentials and data; report concerns immediately; preserve evidence and avoid unauthorised investigation.
Pupils	Follow the age-appropriate pupil agreement; keep passwords private; respect others; avoid harmful content and contact; report anything worrying; use technology only as authorised.
Parents and carers	Support safe use at home; maintain current contacts and consent; report relevant concerns; use official platforms respectfully; avoid publishing information or images concerning other children.



Role	Responsibilities
Contractors volunteers and visitors	Use only authorised access; comply with confidentiality, safeguarding and acceptable-use requirements; report incidents immediately; return access and equipment when work ends.

6 Acceptable and responsible use

6.1 General requirements

School technology must be used for authorised educational, administrative or professional purposes. Limited incidental employee use may be permitted where it does not affect duties, security, safeguarding, cost, performance or the school's interests. All users must:

- Use only their own authorised account and keep authentication details secure.
- Follow staff instructions, age restrictions, platform terms and school controls.
- Communicate respectfully and never bully, threaten, harass, discriminate, impersonate or deliberately humiliate another person.
- Protect confidential and personal information and check recipients before sending.
- Report accidental access to harmful material, suspicious messages, lost devices and security concerns immediately.
- Respect copyright, licensing, intellectual property and academic honesty.
- Keep devices physically secure and use them only in supervised or authorised areas.
- Sign the acceptable-use agreement relevant to their role or age.

6.2 Prohibited activity

Users must not:

- Attempt to bypass filtering, monitoring, passwords, device controls or network restrictions, including through VPNs, proxies or unauthorised hotspots.
- Access, create, store, request, search for or share harmful, illegal, sexual, violent, hateful, extremist or age-inappropriate material.
- Install software, browser extensions, applications or games without authorisation.
- Connect unauthorised devices, storage media or network equipment.
- Share passwords, use another person's account or leave an account unlocked.
- Make unauthorised recordings, screenshots or copies of lessons, meetings, pupils, employees or school information.
- Send spam, chain messages, scams or material intended to cause alarm or disruption.
- Conduct hacking, scanning, credential testing, malware activity or any attempt to damage or disrupt systems.
- Use school systems for unlawful commercial activity, gambling, personal financial transactions or political campaigning.
- Use technology in a way that breaches safeguarding, behaviour, confidentiality, professional-conduct or Qatar legal requirements.



7 Accounts passwords and access permissions

- Every user receives an individual account where the system supports this. Shared accounts are avoided and, where technically unavoidable, are formally approved and tightly controlled.
- Access follows the principle of least privilege: users receive only the information and functions required for their role.
- The IT Manager maintains an access-permissions matrix and records approval for privileged or administrative access.
- Multifactor authentication is required for privileged accounts, remote access and other services where available and proportionate.
- Passwords must meet the school's current technical standard, must not be reused across personal and school services, and must not be written where others can see them.
- Temporary passwords are changed at first use. Suspected compromise results in immediate reset, session revocation and security review.
- Accounts are amended promptly when duties change and disabled immediately when a user leaves or no longer requires access.
- Administrative accounts are separate from everyday accounts and are used only for authorised technical work.
- Access reviews are completed at least termly and for every staff leaver, role change or safeguarding restriction.

8 Network security filtering and monitoring

8.1 Technical protection

The IT Manager will maintain risk-appropriate controls, including firewalls, anti-malware, secure configuration, patching, account protection, encryption where appropriate, backups and filtering. Controls will cover school networks and school-managed devices and will be reviewed when systems, threats or school provision change.

8.2 Filtering

- Filtering must be age-appropriate and must reduce access to illegal, harmful and inappropriate content without unreasonably restricting teaching and learning.
- Filtering categories, exceptions and allow-list requests require recorded authorisation. Staff must not promise pupils access before approval.
- Attempts to bypass controls generate review and may be treated as a safeguarding, behaviour or security incident.
- The IT Manager conducts and records functional checks at least monthly and after significant configuration or provider changes.
- The DSL and IT Manager jointly review whether controls respond adequately to current safeguarding risks at least termly.



8.3 Monitoring

RIS may monitor school networks, accounts, devices and approved platforms for safeguarding, security, compliance and operational purposes. Monitoring must be authorised, transparent, proportionate and limited to legitimate school purposes. Access to monitoring information is role-based and auditable.

- Technical alerts are reviewed by the IT Manager; possible child-safety concerns are referred immediately to the DSL.
- Monitoring information is not used for personal curiosity, general surveillance without purpose or unauthorised investigation.
- Users are informed that school systems may be monitored and that privacy cannot be guaranteed on school-owned systems.
- Significant alerts, patterns and actions are recorded and reported termly to the Executive Principal.

9 Personal data privacy and records

Personal data will be collected, used, shared, stored and deleted only for legitimate school purposes and in accordance with Qatar Law No. 13 of 2016, current official guidance and the RIS Data Protection Policy. The school will apply data minimisation, accuracy, access control, confidentiality, retention and secure disposal.

- Only approved systems may hold pupil, parent, employee, assessment, attendance, medical, financial, identification or safeguarding data.
- Users must verify recipients, attachments and sharing permissions before sending information.
- Sensitive data must not be copied to personal email, personal cloud storage, unapproved messaging services or unauthorised AI tools.
- Privacy notices will explain relevant processing, sharing and individual rights. Consent will be obtained where consent is the appropriate basis for the activity.
- Records are retained according to the approved retention schedule and securely deleted when no longer required.
- Third-party access requires authorisation, confidentiality and data-processing controls appropriate to the risk.
- Cross-border or cloud processing is assessed before approval, including location, safeguards, deletion and access arrangements.
- Requests concerning personal data are referred immediately to the Data Protection Lead and are not answered informally by individual staff.



10 School devices personal devices and removable media

10.1 School devices

- School devices remain school property, may be monitored and must be returned on request.
- Users must not disable security controls, alter configurations or allow unauthorised people to use a device.
- Devices must be locked when unattended and stored securely. Loss, theft or damage is reported immediately.
- Confidential information should not be downloaded locally unless required and authorised. Local copies must be protected and deleted when no longer needed.

10.2 Personal devices and bring your own device arrangements

Pupil personal devices must remain switched off and stored as directed unless a teacher has specifically authorised use for a defined learning or medical purpose. The school may provide a segregated guest network but does not guarantee access for personal devices.

Employees must not use personal devices to photograph, film, record or store information about pupils. Exceptional professional use requires prior written approval from the Executive Principal and DSL, use of an approved application, no permanent local storage and immediate secure transfer and deletion. Personal messaging accounts must not be used for pupil or parent communication.

The School may restrict or withdraw personal-device access where there is a safeguarding, security or operational concern. Any examination or search of a personal device must be authorised, lawful, necessary, proportionate and undertaken under the Safeguarding and Behaviour policies.

10.3 Removable media and charging

- USB drives and other removable storage may be used only when authorised, encrypted where appropriate and scanned for malware.
- Unknown or found media must not be connected to a school device.
- Devices may be charged only with safe, undamaged equipment in approved locations. Personal charging must not create fire, trip or supervision risks.



11 Communication email and social media

- Communication with pupils and parents must use approved school accounts and platforms such as school email, ClassDojo or Microsoft Teams, according to the purpose and relevant school procedure.
- Employees must not accept or initiate social-media connections with current pupils or communicate through personal email, personal telephone numbers or personal messaging accounts.
- Messages must be professional, necessary and capable of appropriate review. One-to-one pupil communication must remain visible or retrievable through the approved system.
- Confidential information, internal documents and pupil information must not be discussed on public or informal group channels.
- Staff must use caution when identifying their employment online and must not present personal views as official school views.
- Parents and pupils must not use school platforms to bully, threaten, identify or criticise children publicly, disclose confidential information or circulate unverified allegations.
- Nothing in this policy prevents lawful safeguarding reports, complaints, protected disclosures or contact with competent authorities through appropriate channels.

12 Images video audio and live streaming

- Pupil images, recordings and identifying information may be created and used only for an approved purpose and in accordance with consent, safeguarding and data-protection requirements.
- School-owned or school-authorised equipment and accounts must normally be used. Personal-device capture or storage is prohibited except under the written exceptional arrangement in section 10.2.
- Group photographs are preferred for whole-school events. Individual pupil features require a clear educational or celebratory purpose and appropriate consent.
- Names, location information, uniforms, metadata and accompanying text are checked so that publication does not create an avoidable identification or safety risk.
- Images and recordings are stored securely, retained only as long as required and removed from publication when consent is withdrawn where this is applicable and practicable.
- Parents and visitors must follow event-specific photography rules and must not publish identifiable images of other children without appropriate permission.
- Live streaming requires prior approval, a host using an approved account, controlled access, appropriate supervision and a clear decision on whether recording is permitted.



13 Online safety education and training

13.1 Pupil education

Online safety will be taught progressively through computing, PSHE/pastoral learning, safeguarding work and relevant curriculum contexts. Planning will be age-appropriate from EYFS to Year 6 and will address:

- Trusted adults and how to ask for help.
- Privacy, personal information, passwords and digital footprints.
- Respectful communication, cyberbullying and consent before recording or sharing.
- Safe searching, harmful content, pop-ups and reporting.
- Unknown contacts, grooming, requests for images and manipulation.
- Scams, advertising, gaming, in-app purchases and gambling risks.
- Misinformation, reliability, copyright and academic honesty.
- Safe, ethical and age-appropriate use of artificial intelligence.
- How school filtering and monitoring help protect users.

Teaching must be adapted for pupils with SEND, communication needs or other vulnerabilities. Staff will avoid frightening content and will use language suited to pupils' developmental stage.

13.2 Staff training

All staff receive online-safety and digital-security induction before or promptly after access is issued, followed by at least annual refresher training and updates when risks or systems change. Role-specific training is provided for the DSL, IT Manager/Data Protection Lead, leaders and employees supervising higher-risk activities. Training attendance and understanding are recorded.

13.3 Parent awareness

RIS will provide regular information to parents on age restrictions, parental controls, gaming, social media, privacy, scams, reporting and emerging risks. Parent communications will make clear that home and school responsibilities are complementary and that concerns affecting a pupil should be reported promptly.

14 Reporting safeguarding and incident response

14.1 How to report

- Pupils may report to any trusted adult. The adult must listen, reassure, avoid blame and pass the concern to the DSL without delay.
- Employees report safeguarding concerns to the DSL and technical or security concerns to the IT Manager. Where both apply, both leads are informed immediately.
- Concerns about an adult's online conduct are reported directly to the Executive Principal or, when the concern relates to the Executive Principal, to the designated Board contact under safeguarding procedures.
- Parents report concerns through the class teacher, DSL or Executive Principal depending on seriousness. An immediate risk should not wait for routine communication hours.
- Any person may contact emergency or competent authorities directly where immediate protection is required.



14.2 Immediate response

1. Protect the pupil or affected person from further contact, exposure or immediate harm.
2. Inform the DSL and, where relevant, the IT Manager and Data Protection Lead.
3. Preserve relevant usernames, URLs, dates, times, messages and device details without unnecessarily viewing, copying or forwarding harmful material.
4. Do not conduct an unauthorised interview, search, deletion or confrontation that could increase risk or compromise evidence.
5. Assess safeguarding, technical, data-protection, behaviour and legal implications and assign a lead person.
6. Inform parents unless doing so could increase risk, compromise an investigation or conflict with authority advice.
7. Refer to competent authorities when required, implement protective action and record the decision and rationale.
8. Review controls, education and supervision and confirm that corrective actions are closed.

15 Cyberbullying and online conduct outside school

RIS may respond to online conduct occurring outside school where it affects a pupil's safety, wellbeing, attendance, relationships or education; involves members of the school community; uses school systems; or creates a safeguarding or operational risk. The response may include safeguarding support, evidence preservation, parent meetings, restorative work, behaviour sanctions, technical restrictions and referral to authorities.

The School will distinguish disagreement or legitimate criticism from bullying, harassment, threats, impersonation, discriminatory abuse, disclosure of private information or coordinated targeting. Actions will be proportionate, consistent and sensitive to pupil age, vulnerability, intent, impact and repetition.

16 Harmful content grooming and sexual imagery

Any concern involving grooming, sexual communication, requests for images, sexual imagery of a child, sextortion, exploitation, extremist material, credible threats, self-harm or suicide content must be reported to the DSL immediately. Staff must not promise confidentiality.

- Do not ask a pupil to send, forward, print or display sexual or illegal material.
- Do not copy or distribute the material. Record what was reported and the location of possible evidence rather than unnecessarily viewing it.
- Secure the device or account only when authorised and necessary to prevent further harm; do not investigate or delete evidence without direction.
- The DSL will assess immediate safety, contact parents when safe and appropriate, and make required referrals to Qatar authorities.
- Pupils affected by harmful or coercive content will receive support and will not automatically be treated as responsible for abuse committed against them.



17 Artificial intelligence

- AI tools may be used only when approved for the user's age, purpose, safeguarding and data-protection risk. AI output is not assumed to be accurate, unbiased, lawful or suitable for pupils.
- Employees must not enter pupil names, Qatar identification numbers, contact details, medical information, safeguarding information, assessment records, photographs, staff-confidential information or unpublished school documents into a public or unapproved AI service.
- Staff remain professionally responsible for checking accuracy, bias, copyright, cultural suitability, age appropriateness and confidentiality before using AI-generated material.
- Pupil use requires teacher approval and supervision. Tasks must state when AI assistance is allowed and how it should be acknowledged.
- AI must not be used to impersonate, create deepfakes, generate harmful or sexualised material, evade assessment, make automated safeguarding decisions or replace professional judgement.
- Any AI platform considered for routine school use must complete the third-party approval process in section 19.
- RIS will review AI practice at least annually because risks, product terms and official expectations change rapidly.

18 Remote learning video conferencing and recordings

- Only approved school accounts and platforms may be used for remote teaching or pupil meetings.
- Invitations and access links must be controlled. Meetings must use appropriate waiting-room, participant and screen-sharing settings.
- Staff must conduct sessions from a professional setting, use appropriate language and dress, and consider whether another adult or parent should be present for younger pupils or one-to-one work.
- Pupils must join from an appropriate shared learning space where possible, use their correct name and follow behaviour expectations.
- Lessons, meetings, screens or chats must not be recorded or captured unless the school has approved the purpose, participants have been informed and data-protection requirements are met.
- Safeguarding disclosures, concerning behaviour or unexpected participants are handled through the normal safeguarding procedure.
- Remote learning does not permit informal personal messaging or communication outside approved channels.



19 Third party systems and cloud services

- No employee may require pupils, parents or colleagues to use a new application, website, AI tool or cloud service until it has been approved. The approval record will consider.
- Educational or operational purpose and whether an existing approved system already meets the need.
- Provider identity, reputation, security arrangements and support.
- Age restrictions, parental information and pupil-account requirements.
- Data collected, legal purpose, advertising, tracking, profiling and use for product or AI-model training.
- Data storage location, international processing, subcontractors and access controls.
- Contract terms, confidentiality, breach notification, deletion and return of information.
- Accessibility, cultural appropriateness and content controls.
- Exit arrangements so that school information can be retrieved and securely deleted.

The IT Manager maintains an approved systems and suppliers register. High-risk processing requires documented privacy and security assessment and approval from the Executive Principal and DSL as applicable.

20 Cyber incidents personal data breaches and continuity

20.1 Examples

Incidents include phishing, malware, ransomware, account compromise, unauthorised access, loss or theft of a device, misdirected information, accidental publication, unauthorised recording, website defacement, service outage, inappropriate access by an employee or supplier and loss of personal data.

20.2 Response

1. Report immediately to the IT Manager and Data Protection Lead. Safeguarding implications are also reported to the DSL.
2. Contain the incident without destroying evidence. Disconnect an affected device from networks if instructed; do not power off, wipe or reset unless directed.
3. Record the time, systems, accounts, people, information and actions involved.
4. Secure accounts, sessions, access keys and affected services; preserve logs and relevant communications.
5. Assess impact on confidentiality, integrity, availability, pupil safety and school operations.
6. Notify the Executive Principal, insurer, service provider and competent authorities as required. Notification is made without delay and within any period set by the applicable authority.
7. Communicate accurately with affected people when required and safe, without compromising safeguarding or investigation.
8. Recover from verified backups, monitor for recurrence and complete a documented review and corrective-action plan.



20.3 Business continuity

- Critical systems and data will be identified and backed up according to documented schedules.
- Backups will be protected from ordinary user access and tested through documented restoration exercises.
- The Crisis and Emergency Management Plan will address loss of connectivity, management systems, communications and access to essential safeguarding information.
- Alternative communication and attendance arrangements will be available when primary systems are unavailable.

21 Investigation sanctions and restoration

Incidents will be managed under safeguarding, behaviour, staff conduct, data protection and health and safety procedures as appropriate. The school may restrict or suspend access while risk is assessed. Any investigation must be authorised, fair, confidential and proportionate.

- Pupil responses may include education, pastoral support, restorative action, increased supervision, parental involvement, access restrictions and proportionate Behaviour Policy sanctions.
- Employee concerns may result in management instruction, retraining, access restriction or formal action under applicable conduct procedures.
- Contractor or visitor access may be withdrawn and the employer or relevant authority informed.
- Deliberate illegal, abusive or seriously harmful conduct may be referred to competent Qatar authorities.
- Access is restored only when risk controls are in place and the responsible leader has authorised restoration.
- Victims and affected pupils receive appropriate safeguarding and pastoral support irrespective of any sanction applied to another person.



22 Monitoring assurance and evidence

The School will demonstrate implementation through records rather than relying on the existence of the policy alone.

Frequency	Assurance activity	Evidence
Ongoing	Record incidents, safeguarding referrals, technical alerts, data breaches, access changes, system approvals and corrective actions.	Incident logs; safeguarding records; service tickets; breach register; approvals.
Monthly	Check filtering function, critical updates, malware status, backups, privileged accounts and expiring system or security controls.	Signed technical checklist; exception and action log.
Termly	Joint DSL and IT review of patterns; user access review; sample acceptable-use compliance; curriculum and training review; report to SLT and Board.	Termly report; access matrix; curriculum evidence; training matrix; action tracker.
Annually	Policy review; pupil, parent and staff awareness; supplier and platform review; restoration exercise; review of risk assessments and privacy notices.	Approved policy; survey/feedback; supplier register; test report; updated risk assessments.
After a serious incident or material change	Debrief, root-cause review, safeguarding review, control testing and confirmation that actions are effective.	Incident review; notifications; revised risk assessment; closure evidence.

The minimum evidence portfolio will include signed acceptable-use agreements, staff training, pupil curriculum records, parent awareness communications, filtering and monitoring checks, access reviews, device and software inventory, approved platforms register, incident and breach records, image consent, backup restoration evidence and completed action plans.



23 Complaints review and approval

Concerns about this policy or its implementation should be raised with the Executive Principal. Safeguarding or security reports must not be delayed while a complaint is considered. Formal complaints follow the School Complaints Policy, and lawful protected disclosures remain unaffected.

This policy is reviewed at least annually and sooner following a serious online-safety or cyber incident, significant system change, audit finding, new AI or monitoring practice, or change in Qatar requirements. The DSL, IT Manager and Data Protection Lead contribute to the review. The Executive Principal confirms implementation and the Board of Directors approves the policy.



Appendix A Staff acceptable use agreement

I understand that access to RIS systems and information is provided for authorised professional purposes and is conditional on compliance with this policy, safeguarding procedures and the Staff Code of Conduct.

I agree that I will:

- Use only authorised accounts, devices, platforms, software and storage.
- Protect passwords, use multifactor authentication where required and lock devices when unattended.
- Keep pupil, parent, employee and school information confidential and send it only to verified authorised recipients.
- Communicate with pupils and parents only through approved school channels.
- Not photograph, film or record any pupil where consent has not been given.
- Not enter confidential, personal or safeguarding information into an unapproved AI or online service.
- Supervise pupils appropriately and pre-check digital resources for age and cultural suitability.
- Report safeguarding, harmful-content, phishing, malware, loss, misdirection and data-breach concerns immediately.
- Preserve evidence and not conduct an unauthorised investigation or deletion.
- Follow copyright, licensing, records-retention and secure-disposal requirements.
- Return school devices and cease access when requested or when my role ends.
- Accept proportionate monitoring of school systems for safeguarding, security and compliance.

Agreement	Details
Employee name	
Role	
Signature	
Date	



Appendix Key Stage 1 Pupil agreement

These rules should be explained to the pupil in age-appropriate language. A parent or carer should acknowledge the agreement.

- I use school technology only when an adult tells me I may use it.
- I keep my name, address, passwords and family information private.
- I am kind and respectful when I use technology.
- I do not take photographs or recordings unless a teacher says it is allowed.
- I stop and tell a trusted adult if something makes me worried, upset or confused.
- I do not click pop-ups, messages or links I do not understand.
- I ask before downloading, buying or joining anything online.
- I know I will not be in trouble for telling an adult about something worrying.

Acknowledgement	Details
Pupil name and class	
Parent or carer name	
Parent or carer signature	
Date	



Appendix C Key Stage 2 pupil acceptable use agreement

- I understand that school technology is provided to help me learn and that the school may check activity on its systems to keep people safe.
- I use only my own account and keep my password private.
- I use websites, applications, email, ClassDojo, Teams and AI only when my teacher allows them.
- I do not try to bypass filters, use VPNs or change device settings.
- I communicate kindly and do not bully, threaten, impersonate or share embarrassing content.
- I protect my personal information and do not arrange to meet an online contact.
- I ask permission before photographing, recording or sharing information about another person.
- I check information carefully, respect copyright and say when I have used AI or another person's work.
- I do not enter anyone's private information into AI tools, games, websites or applications.
- If I see harmful content, receive an unwanted message or make a mistake, I close or move away when safe and tell a trusted adult immediately.
- I understand that access may be restricted and school procedures followed if I break these rules.

Agreement	Details
Pupil name and class	
Pupil signature	
Parent or carer name and signature	
Date	



Appendix D Online safety incident response card

- Protect the pupil or affected person from immediate contact, exposure or harm.
- Report to the DSL. Also inform the IT Manager for technical concerns and possible personal-data loss or disclosure.
- Record what was reported, by whom, when, the platform, account, URL and device. Preserve evidence without unnecessarily viewing or forwarding harmful material.
- Do not promise confidentiality, confront the alleged person, delete accounts or conduct an unauthorised device search.
- Assess immediate safeguarding, technical and privacy risk and decide whether parents and competent authorities should be contacted.
- Implement protective measures, support the pupil and record decisions, referrals and communications.
- Review filtering, supervision, access, training and curriculum implications and verify completion of actions.

Immediate danger or credible threat. Contact the appropriate emergency service or competent Qatar authority without waiting for the routine school process.



Appendix E Cyber incident and data breach checklist

Stage	Required checks
Report and protect	☐ IT Manager/Data Protection Lead informed ☐ DSL informed if child-related ☐ Executive Principal informed according to severity ☐ Immediate safety action taken
Contain	☐ Affected account/session secured ☐ Device/network isolated if directed ☐ Passwords/keys reset ☐ Supplier contacted ☐ Evidence and logs preserved
Assess	☐ Data and people identified ☐ Confidentiality impact ☐ Integrity impact ☐ Availability impact ☐ Safeguarding impact ☐ Operational impact ☐ Continuing threat
Notify	☐ Parent/individual decision recorded ☐ Board/insurer/provider informed ☐ Authority notification considered/completed ☐ Communication approved and recorded
Recover	☐ Systems cleaned/verified ☐ Backup restored and tested ☐ Access reviewed ☐ Monitoring increased ☐ Normal operation authorised
Review	☐ Root cause recorded ☐ Actions assigned ☐ Risk assessment updated ☐ Training/policy/control updated ☐ Effectiveness checked ☐ Incident formally closed



Appendix F Termly compliance audit and evidence schedule

Check	Evidence	Complete and action
Policy approved current and communicated	Approved policy; distribution and acknowledgement records	☐ Action: _____
Staff pupil and contractor acceptable-use agreements current	Signed agreements and exceptions register	☐ Action: _____
Filtering active and tested	Monthly tests; category and exception review	☐ Action: _____
Monitoring alerts reviewed and escalated correctly	Alert sample; DSL and IT review record	☐ Action: _____
Firewall anti-malware patching and backups current	Technical dashboard/checklist; restoration test	☐ Action: _____
User access matches current roles and leavers removed	Access matrix; joiner mover leaver audit	☐ Action: _____
Privileged accounts and multifactor authentication reviewed	Admin account register and access review	☐ Action: _____
Devices software and licences recorded	Current inventory; authorised software list	☐ Action: _____
Third-party and cloud systems remain approved	Supplier register; privacy/security assessments	☐ Action: _____
Pupil online-safety curriculum delivered	Plans; lesson evidence; pupil work or evaluation	☐ Action: _____
Staff training current and effective	Training matrix; induction and refresher evidence	☐ Action: _____
Parent awareness activity completed	Messages; workshop or guidance records	☐ Action: _____
Image consent and publication controls sampled	Consent register; website/social-media sample	☐ Action: _____
Incidents and data breaches analysed for trends	Incident log; breach register; termly analysis	☐ Action: _____



Check	Evidence	Complete and action
Corrective actions closed and checked	Action tracker with effectiveness evidence	☐ Action: _____
Termly assurance reported to SLT and Board	Minutes; report; decisions and follow-up	☐ Action: _____

Reference sources

- Ministry of Education and Higher Education, Guidelines for the Mandatory Evaluation Process for Private Schools 2026 – school-supplied English translation.
- Qatar Law No. 13 of 2016 on Protecting Personal Data Privacy:
<https://www.almeezan.qa/EnglishLaws//132016.pdf>
- National Cyber Security Agency, Personal Data Privacy Protection guidance:
<https://ncsa.gov.qa/en/pages/governance-assurance-personal-data-privacy>
- UK Department for Education, Keeping Children Safe in Education 2026:
<https://www.gov.uk/government/publications/keeping-children-safe-in-education--2>

Reference review date: 16 September 2026. The latest Qatar law, official circular or authority direction must be followed where it is more recent or more specific than this policy.