



GEMS

مدرسة جيمس وينشستر

Winchester School

ABU DHABI

Online Safety (E-Safety) Policy

UPDATED BY	LAST PUBLISH DATE	MONITORING CYCLE
Dr.Karon Buck	September 2025	September 2026

1. Introduction

GEMS Winchester School - Abu Dhabi opened in 2013 and offers the National Curriculum for England from Foundation Stage to Year 9. The school provides a secure, caring and personalised learning environment, enhanced by constructive communication with parents and caregivers, to enable every student to flourish academically, socially and personally.

Digital technology is an essential part of learning, communication and school operations. The school recognises that technology creates opportunities for creativity, collaboration, independent thinking and achievement, but also introduces safeguarding, wellbeing, conduct, data protection and cybersecurity risks. This policy sets out how GEMS Winchester School - Abu Dhabi protects students, supports staff and families, and promotes responsible, ethical and safe digital participation.

Online safety is treated as a safeguarding responsibility. All members of the school community are expected to act in the best interests of students, uphold zero tolerance of maltreatment, and report concerns without delay through the appropriate safeguarding and digital incident procedures.

2. Purpose and Aims

The purpose of this policy is to establish clear, consistent and ADEK-compliant expectations for online safety, responsible technology use and digital safeguarding across GEMS Winchester School - Abu Dhabi.

- Safeguard students from online harm, including the 4Cs of online risk: content, contact, conduct and commerce.
- Promote digital citizenship, digital fluency, academic honesty, online respect and positive behaviour.
- Set clear rules for the safe and responsible use of school networks, school devices, personal devices, approved learning applications, artificial intelligence tools and digital communications.
- Ensure robust filtering, monitoring, cybersecurity, incident response and record-keeping arrangements supported by trained human oversight.
- Support parents and caregivers with practical digital parenting guidance, including age-appropriate monitoring and open communication.
- Ensure that online safety practice is aligned with GEMS safeguarding expectations, ADEK school policy requirements, UAE law and school-specific policies.
- Provide clear escalation routes for digital incidents, safeguarding concerns, cyberbullying, youth-produced sexual imagery, online challenges, data breaches and cybersecurity incidents.

3. Scope

This policy applies to all students, staff, parents/caregivers, Local Advisory Board members, volunteers, visitors, contractors, invited visitors and external providers who use, access or interact with school systems, devices, networks or school-related digital spaces.

The policy applies in the following contexts:

- on school premises, including classrooms, corridors, learning spaces, offices, libraries, shared areas and reception areas;
- on school networks, school-managed devices, school cloud services, learning platforms, email, Microsoft Teams, Seesaw and any approved system;
- on personal devices used under school direction, BYOD arrangements or to access school systems;
- during lessons, break times, extracurricular activities, off-site visits, transport, events, distance learning and virtual interactions;
- on official school social media, digital media and communication channels;
- where online behaviour outside school creates a safeguarding concern, disrupts learning, damages the school community, involves school members, or requires school intervention under ADEK, GEMS or UAE requirements.

4. Regulatory and Policy Framework

This policy has been written to align with the current school, GEMS and ADEK requirements relevant to online safety, student protection, safeguarding, digital use and cybersecurity. It must be read in conjunction with the following:

- GEMS Safeguarding / Student Protection Policy 2025-26 and GEMS safeguarding case-management expectations.
- GEMS Safer Working Practice Guidance, Staff Code of Conduct and relevant GEMS information security guidance.
- GEMS Winchester School - Abu Dhabi school policies, including BYOD Policy 2025, Behaviour Policy, Anti-Bullying Policy, Inclusion Policy, Educational Risk Policy, Learner Mental Health and Wellbeing Policy, Parent Handbook, cybersecurity guidance for parents and students, and related acceptable-use agreements.
- ADEK School Digital Policy, including requirements for responsible usage policies, digital safeguarding, student digital competencies, digital infrastructure, cybersecurity, data protection, digital media, social media, personal staff social media and incident recording.
- ADEK School Safeguarding Policy and ADEK School Student Protection Policy, including the best interests of students, zero tolerance of maltreatment, duty of care, safeguarding governance, training, awareness, online-space vigilance and record keeping.

GEMS Winchester School, Abu Dhabi

Madinat Zayed

+971 (02) 403 5499

<http://gemswinchesterschool-abudhabi.com/>

WSA Investing In YOU!

- Relevant UAE laws and regulatory requirements, including Federal Decree Law No. 3 of 2016 Concerning Child Rights (Wadeema), Federal Decree Law No. 18 of 2020 on Private Education and its amendments, Federal Decree Law No. 34 of 2021 on Combatting Rumors and Cybercrimes, Federal Decree Law No. 38 of 2021 on Copyrights and Related Rights, Federal Decree Law No. 45 of 2021 on the Protection of Personal Data, and any applicable ADEK circulars or instructions.

5. Definitions

Term	Definition
Online safety / e-safety	The safe, responsible and ethical use of digital technology, the internet, communication tools, digital media, artificial intelligence and online services.
Digital device	Any device used for audio, video, text communication, computing or internet access, including laptops, tablets, school devices, mobile phones, smart watches and other connected devices.
Digital incident	Any inappropriate use of digital technology, including breach of responsible use rules, accessing inappropriate content, inappropriate online behaviour or communication, cyberbullying, use of VPNs to bypass controls, or any breach of school rules in an online setting.
Digital safeguarding	The systems, education, procedures and culture used to protect students from online harm and to respond to concerns in a timely, proportionate and child-centred way.
Filtering	Technical measures used to block access to harmful, illegal, inappropriate or non-educational content on school-managed networks and devices.
Monitoring	Reviewing network, device or system activity to identify risk, misuse or harm. Monitoring is proportionate, safeguarding-led, recorded and overseen by authorised staff.
CPC/DSL	Child Protection Coordinator / Designated Safeguarding Lead, the senior leader responsible for safeguarding and child protection, including online safety and filtering/monitoring oversight.
DDSL / Deputy CPC/DSL	Deputy safeguarding lead trained to support and act in the absence of the CPC/DSL.
Digital Safety Lead / ICT Engineer	The member of staff responsible for technical online safety arrangements, secure infrastructure, filtering, monitoring support, incident response and liaison with senior leaders and ADEK where required.
Youth-produced sexual imagery (YPSI)	Sexual imagery created, shared or possessed by children or young people. It is always managed as a safeguarding concern.

Term	Definition
Artificial intelligence (AI)	Digital systems that generate, analyse, recommend, classify or transform content, including chatbots, generative text, image, audio/video tools, adaptive learning and analytics tools.

6. Policy Principles

- The best interests, dignity, wellbeing and safety of students are the primary consideration in all online safety decisions.
- Every staff member, volunteer and service provider has a responsibility to recognise, respond to and report online safety and safeguarding concerns. Staff do not investigate safeguarding concerns themselves.
- Online safety is everyone's responsibility and is embedded through curriculum, pastoral care, safeguarding, behaviour, cybersecurity, parent engagement and student voice.
- The school will provide age-appropriate, inclusive online safety education and accessible guidance for students, including students with additional learning needs.
- The school will maintain effective technical controls, but recognises that filtering and monitoring do not replace education, professional vigilance, parental partnership and student responsibility.
- The school will act proportionately, supportively and restoratively where appropriate, while applying sanctions and referrals where behaviour creates risk, harm, illegality or a serious breach of trust.
- Confidential information and safeguarding records are shared on a need-to-know basis only and handled in accordance with GEMS and ADEK requirements.

7. The 4Cs of Online Safety

The school educates students, staff and families to recognise and respond to four broad categories of online risk. These categories are used in curriculum planning, parent guidance, incident triage and safeguarding responses.

Area	Student role	Risk examples	School response
Content	Child as recipient	Illegal, inappropriate or harmful online material, including explicit adult content, racism, misogyny, radicalisation, extremism, misinformation, self-harm or suicide content, violent content, conspiracy theories and age-inappropriate material.	Filtering, curriculum education, reporting routes, pastoral support, parent engagement, safeguarding escalation where risk or harm is identified.
Contact	Child as participant	Harmful online interaction with others, including fake profiles, strangers, grooming, exploitation, peer pressure,	Students are taught how to block, report and seek help. Concerns are reported to the CPC/DSL, logged on

GEMS Winchester School, Abu Dhabi

Madinat Zayed

+971 (02) 403 5499

<http://gemswinchesterschool-abudhabi.com/>

WSA Investing In YOU!

Area	Student role	Risk examples	School response
		targeted advertising, coercion, bullying or manipulation.	Guard where safeguarding-related, and escalated externally where required.
Conduct	Child as actor	Online behaviour that may harm self or others, including cyberbullying, sharing images without consent, oversharing, impersonation, online challenges, harassment, accessing or distributing prohibited content, and misuse of AI.	Behaviour, anti-bullying, safeguarding and restorative responses are applied. Serious or repeated conduct is escalated to SLT, parents and external agencies where necessary.
Commerce	Child as consumer	Financial and data risks including phishing, scams, in-game purchases, online gambling, inappropriate advertising, data harvesting, fake competitions, subscription traps and identity theft.	Cybersecurity education, restrictions on payment activity, data protection controls, reporting to IT/DSL and parent guidance are used to reduce risk.

8. Roles and Responsibilities

8.1 Principal and Senior Leadership Team

- Hold overall responsibility for a culture of safeguarding, including online safety, digital behaviour and cybersecurity.
- Ensure that the CPC/DSL, Deputy CPC/DSL, Digital Safety Officer, ICT Engineer and relevant staff have the training, authority and resources to fulfil their responsibilities.
- Ensure serious digital incidents, safeguarding concerns and cyber incidents are responded to promptly and reported to ADEK, GEMS Central Safeguarding Team, Police, Family Care Authority or other authorities where required.
- Ensure that every digital incident requiring school action is recorded, documented, signed by the Principal where required, and stored for audit in line with ADEK and school records procedures.
- Ensure digital safety is embedded in curriculum planning, induction, staff training, parent communication and student support.
- Approve school digital media, official social media, external learning applications, virtual visitor arrangements and any exceptional use of personal devices where required.

8.2 CPC/DSL and Deputy CPC/DSL

- Lead day-to-day safeguarding responses to online safety concerns and ensure online safety is integrated with student protection procedures.
- Maintain Level 3 safeguarding training and attend required GEMS and ADEK updates.

GEMS Winchester School, Abu Dhabi

Madinat Zayed

+971 (02) 403 5499

<http://gemswinchesterschool-abudhabi.com/>

WSA Investing In YOU!



- Understand the school's filtering and monitoring systems and work with ICT staff to review concerns and patterns of risk.
- Ensure safeguarding concerns are recorded accurately on Guard without undue delay, with actions, decisions and outcomes documented.
- Ensure students who are harmed, vulnerable or at risk online receive timely support and, where appropriate, referral.
- Advise staff on reporting, evidence preservation, student conversations, parent communication and external referrals.
- Ensure child-on-child abuse, youth-produced sexual imagery, online exploitation, grooming, self-harm content, radicalisation/extremism concerns and serious cyberbullying are managed as safeguarding matters.

8.3 Digital Safety Lead / ICT Engineer

- Maintain secure digital infrastructure, filtering, monitoring, network security, endpoint protection, access control and technical incident response.
- Ensure users access systems through secure authentication, appropriate passwords, role-based permissions and multi-factor authentication where required for critical services.
- Ensure web filtering policies are enforced, inappropriate content can be blocked, network activity can be monitored and logs are maintained for audit and safeguarding review.
- Report safeguarding-related digital alerts or misuse to the CPC/DSL without delay and technical/cybersecurity incidents to SLT in accordance with incident response procedures.
- Maintain appropriate security controls, including antivirus/anti-malware, patching, encryption, backups, data loss prevention, cloud security, intrusion prevention/detection and disaster recovery arrangements.
- Support risk assessment of third-party digital providers, applications, open-source tools and AI tools, including data security, age-appropriateness and educational suitability.
- Liaise with ADEK on digital competency, safety and security matters where assigned by the Principal.

8.4 Teaching and Support Staff

- Read, understand and comply with this policy, the Staff Code of Conduct, GEMS safeguarding expectations and acceptable use requirements.
- Model safe, respectful and professional digital behaviour at all times.
- Use only approved school systems for school communication, teaching, storage and sharing of student information.
- Never use personal email, personal social media or private messaging applications to communicate with current students. Communication with parents must take place through approved school channels unless explicitly authorised by SLT for a specific purpose.

GEMS Winchester School, Abu Dhabi

Madinat Zayed

+971 (02) 403 5499

<http://gemswinchesterschool-abudhabi.com/>

WSA Investing In YOU!



- Maintain professional boundaries and report any incident that could be misinterpreted or could create safeguarding risk.
- Embed online safety in lessons and monitor student use of devices, platforms, cameras and digital tools.
- Report all online safety and safeguarding concerns to the CPC/DSL as quickly as possible and record on Guard where appropriate. Staff must not leave site with an undisclosed safeguarding concern.
- Do not investigate safeguarding concerns independently, promise confidentiality or view, save, forward, print or share illegal or suspected illegal content.

8.5 Students

- Use school systems, networks and devices responsibly, safely and for educational purposes.
- Follow this policy, the Digital Device Responsible Use Agreement, the BYOD Policy, behaviour expectations and teacher instructions.
- Report online worries, harmful content, cyberbullying, unsafe contact, scams, online challenges or misuse to a trusted adult without delay.
- Do not access, search for, create, share, store or distribute harmful, illegal, offensive, sexual, violent, discriminatory, bullying or age-inappropriate content.
- Do not use VPNs, hotspots, proxy services or other methods to bypass school filtering, monitoring or security controls.
- Do not take, record, transmit, post or share photos, videos or audio of any member of the school community without explicit permission and consent.
- Protect passwords and personal data, respect the privacy and dignity of others, and behave online with kindness, integrity and honesty.

8.6 Parents and Caregivers

- Support the school's online safety expectations, responsible use agreements and BYOD requirements.
- Monitor students' use of digital devices outside school premises and school hours and encourage safe, age-appropriate online behaviour.
- Maintain open dialogue with children about online activity, contacts, privacy, digital wellbeing and how to seek help.
- Report school-related online safeguarding concerns, cyberbullying, inappropriate contact or harmful content to the school promptly.
- Attend or engage with parent guidance, workshops, communications and digital parenting resources provided by the school.
- Avoid sharing confidential school, staff, parent or student information in unofficial social media or messaging groups.

GEMS Winchester School, Abu Dhabi

Madinat Zayed

+971 (02) 403 5499

<http://gemswinchesterschool-abudhabi.com/>

WSA Investing In YOU!

8.7 Visitors, Volunteers, Contractors and External Providers

- Use only authorised guest access and comply with school visitor, safeguarding, photography, confidentiality and acceptable-use requirements.
- Do not photograph, video, record or publish students or school activity unless explicitly authorised by the Principal and covered by parental consent and school procedures.
- Ensure any digital activity with students is approved, supervised and risk-assessed. Invited virtual interactions must have parental consent and ADEK approval where required.
- Report any online safety or safeguarding concern to the supervising staff member or CPC/DSL immediately.

9. Education, Curriculum and Digital Citizenship

Online safety education is delivered through the curriculum, assemblies, pastoral programmes, ICT/digital learning, wellbeing lessons, campaigns, safer internet activities and responsive teaching following incidents or emerging risks.

9.1 Student Learning

- Students receive age-appropriate teaching on the 4Cs of online safety, cyberbullying, reporting, consent, privacy, respectful communication, digital footprint, misinformation, scams, phishing, password safety, copyright, AI, online challenges and digital wellbeing.
- Students are taught how to block, report and seek help on platforms, how to preserve evidence safely, and how to speak to a trusted adult.
- Digital competencies and expected outcomes are integrated by year group and adapted for students with additional learning needs.
- Younger students up to Grade 6 / Year 7 receive age-appropriate versions of responsible use expectations, with parents receiving the full policy.

9.2 Staff Training

- All staff receive online safety and safeguarding training during induction and through ongoing professional development.
- Training includes the 4Cs, child-on-child abuse, cyberbullying, AI risks, online challenges, YPSI, digital evidence, filtering and monitoring arrangements, data protection, cybersecurity and reporting procedures.
- The CPC/DSL and Deputy CPC/DSL complete required safeguarding training and updates. ICT staff receive role-specific training on secure digital infrastructure, monitoring, incident response and data protection.

9.3 Parent Education and Digital Parenting Partnership

The school recognises digital parenting as a shared responsibility between school and families. Parents are supported through workshops, webinars, newsletters, digital guides, parent meetings, Safer Internet Day activities and targeted communication when trends or risks emerge.

GEMS Winchester School, Abu Dhabi

Madinat Zayed

+971 (02) 403 5499

<http://gemswinchesterschool-abudhabi.com/>

WSA Investing In YOU!

Digital Parenting Step	Expectation
Step 1: Open Communication	Talk regularly with your child about the digital world, possible risks, family boundaries, how to ask for help and the principle of help first, consequences later.
Step 2: Understanding the Risks	Stay informed about online risks using the 4Cs framework, school guidance, specialist resources and ongoing conversations with your child.
Step 3: Modelling Digital Behaviour	Demonstrate balanced, kind, responsible and respectful digital behaviour. Prioritise real-life interaction and healthy digital routines.
Step 4: Parental Control	Use age-appropriate parental controls, privacy settings, app permissions and content filters to reduce exposure to harm.
Step 5: Monitoring Digital Interactions	Monitor online interactions transparently and proportionately, balancing safety, maturity and privacy. Agree arrangements with your child where appropriate.

10. Responsible Use of Technology

Responsible use expectations apply to all school users and are supported by age-appropriate acceptable use agreements. Breach of these expectations may lead to education, pastoral intervention, loss of access, disciplinary action, safeguarding referral or external reporting.

10.1 School Systems, Accounts and Passwords

- School accounts must be used only by the authorised user and must not be shared.
- Passwords must be strong, kept confidential and changed if compromise is suspected.
- Users must log out of shared devices and must not access another person's account, files, messages or data.
- Access to systems is role-based and restricted to the minimum necessary for learning, safeguarding or operational purposes.
- Multi-factor authentication is implemented for critical services where required and appropriate.

10.2 School Network and Internet Use

- School network and internet access are provided for learning, safeguarding, administration and approved school business.
- Users must not attempt to bypass filtering or monitoring, use VPNs or proxies, use unauthorised hotspots, alter network settings, introduce malware, hack systems or interfere with school infrastructure.
- Users must not access or distribute illegal, harmful, offensive, discriminatory, violent, sexual, extremist or age-inappropriate material.



- All users should understand that activity on school systems and networks may be filtered, monitored and logged for safety, security and audit purposes.

10.3 Personal Devices, Mobile Phones, Smart Technology and BYOD

- Personal devices are permitted only where authorised under the WSA BYOD Policy or by the Principal/SLT for a specific educational, medical, accessibility or administrative purpose.
- Under the WSA BYOD expectations, approved student devices may include iPads, tablets and laptops. Gaming devices and mobile/smart phones are not permissible for BYOD unless an explicit exception has been approved.
- Devices may be used only under teacher direction and for curriculum-relevant activity. Use during break times, between lessons or outside the directed learning purpose is not permitted unless permission has been granted for learning, accessibility or wellbeing reasons.
- Students must not use personal devices to record, transmit, post or share images, video or audio of any person on campus or during school activities without explicit permission and consent.
- Social media sites, VPNs and attempts to bypass network security are strictly prohibited on school premises and school networks.
- Students and parents are responsible for the security, charging, insurance and safe use of personal devices. The school is not responsible for loss, theft, damage, data loss or charges incurred on personal devices.
- Where a device is suspected of causing a technical problem, security incident or policy breach, the school may act in accordance with the BYOD Policy, Behaviour Policy, Student Protection Policy, UAE law and safeguarding procedures. Parents will be informed where required and external agency advice will be followed where illegal content or serious risk is suspected.

10.4 External Applications, Cloud Services and Third-Party Providers

- Only approved learning applications, platforms and cloud services may be used for school learning or school data.
- New external tools must be risk assessed for educational value, age-appropriateness, compatibility, accessibility, data protection, cybersecurity, vendor reliability, backup/recovery, storage location and compliance with UAE and ADEK requirements.
- Students must not create accounts for school learning tools using personal details unless approved and consented to in accordance with school procedures.
- Staff must not upload student personal data to external apps, AI tools, cloud storage or websites unless the tool has been approved and the data-sharing basis is lawful and documented.

10.5 Academic Honesty, Copyright and Digital Tools

- Digital tools, including AI, must be used in line with academic honesty, copyright, assessment and teacher instructions.
- Students must not present another person's work, generated content or AI output as their own.
- Users must respect copyright, licensing and fair use expectations when using images, text, audio, video, software or online resources.
- Any required acknowledgement of digital or AI assistance must be completed honestly and in line with school and assessment guidance.

11. Artificial Intelligence and Emerging Technologies

AI can support learning, creativity and accessibility when used safely, ethically and under appropriate supervision. It can also create risks, including inaccurate information, bias, plagiarism, deepfakes, impersonation, harmful generated content, data leakage, age-inappropriate interaction and over-reliance.

- AI tools may be used only for approved educational purposes and in line with teacher instructions.
- Students must not use AI to create or distribute harmful, explicit, discriminatory, bullying, extremist, misleading, impersonating or non-consensual content, including deepfake images, audio or video.
- Personal, confidential, safeguarding, medical or sensitive information about any student, parent, staff member or school matter must not be entered into AI tools unless the tool has been formally approved for that purpose and data protection requirements have been met.
- Students and staff must critically evaluate AI outputs for accuracy, bias, appropriateness, cultural sensitivity and copyright issues before use.
- Staff must risk-assess AI tools before introducing them to students and must consider age restrictions, data use, safeguarding, accessibility and inclusion.
- AI misuse is treated under this policy, the Behaviour Policy, Safeguarding Policy, Staff Code of Conduct and, where relevant, UAE law.

12. Digital Communications, Images, Recording and Social Media

12.1 Staff-Student and Staff-Parent Communication

- Communication between staff and students must take place only for educational or safeguarding purposes using official school-approved systems.
- Staff must not use personal email addresses, personal social media accounts or private messaging applications such as WhatsApp, Telegram or Signal to communicate with current students.
- Staff communication with parents must take place through approved school channels unless a specific exception is authorised by SLT for operational or emergency reasons.

GEMS Winchester School, Abu Dhabi

Madinat Zayed

+971 (02) 403 5499

<http://gemswinchesterschool-abudhabi.com/>

WSA Investing In YOU!

- All communication must be professional, transparent, courteous, purposeful and capable of oversight by senior leaders where required.
- Any communication that becomes concerning, inappropriate, misunderstood or boundary-blurring must be reported to the CPC/DSL or line manager.

12.2 Images, Video, Audio and Digital Media

- Written parental consent must be obtained before recording or publishing photographs, video or audio of students. Consent must explain the purpose and whether the student will be identified by name.
- Parents must be able to withdraw consent through school procedures. The school must maintain accurate consent records.
- Digital media must be stored securely, used only for approved purposes and deleted or archived in line with school records and data protection procedures.
- Personal devices and personal accounts must not be used by staff to capture, store or publish student images or school content, except where a specific, risk-assessed exception has been authorised by the Principal and data protection requirements are met.
- Students must not photograph, record, post, tag or share images, video or audio of others without permission and consent.
- School staff must not take photographs of suspected injuries to students for safeguarding evidence. Where photographic evidence is required, this will be managed by Police, external medical professionals or child protection services in accordance with safeguarding procedures.

12.3 Official School Social Media and Website

- Official school social media accounts and website content are managed only by authorised staff.
- Access, passwords and posting permissions for official accounts are controlled, secure and regularly reviewed.
- Content must be accurate, respectful, culturally appropriate, consented where it involves students, and aligned with GEMS, ADEK and UAE expectations.
- Moderators review, pre-approve or remove third-party content where possible and respond to trolling, bullying, discrimination, harassment, impersonation or inappropriate comments.
- The school monitors official and, where accessible or brought to its attention, unofficial school-related communication channels for safeguarding, bullying or reputational risk.

12.4 Staff Personal Social Media

- Staff must not use school email addresses to create personal social media accounts.
- Staff must use the tightest possible privacy settings and assume all posts may become public and searchable.

GEMS Winchester School, Abu Dhabi

Madinat Zayed

+971 (02) 403 5499

<http://gemswinchesterschool-abudhabi.com/>

WSA Investing In YOU!

- Staff must not send or accept friend, follow or connection requests from current students or former students under 18, and must not use personal social media or messaging apps to communicate with them.
- Staff must not accept parent connection requests on personal social media accounts or use such accounts to communicate with current parents.
- Staff must not share confidential school information, student information, parent information, images, allegations, complaints, internal matters or views that could reasonably appear to be endorsed by the school.
- Staff online conduct must not amount to bullying, harassment, discrimination, intimidation or conduct contrary to UAE cultural values, GEMS expectations or the Staff Code of Conduct.

13. Filtering, Monitoring and Secure Digital Infrastructure

The school maintains a layered Digital Safeguarding and Cybersecurity approach. Technical controls are implemented to protect students, staff, data, systems and the school community, while ensuring that students can access appropriate learning resources.

Control Area	School Expectation
Filtering	Web filtering is enforced to block inappropriate, harmful, illegal or non-educational content. Filtering categories are reviewed and adjusted when risks emerge or legitimate learning needs require review.
Monitoring and logging	Network and system logs are used to detect risks, misuse, cyber threats and safeguarding concerns. Monitoring is proportionate, secure and reviewed only by authorised staff.
Access control	Role-based access is used so users have appropriate permissions. Critical systems use secure authentication and multi-factor authentication where required.
Endpoint protection	School-managed devices are protected with anti-virus/anti-malware software, security updates, patching and hard disk encryption where appropriate.
Network security	Firewalls, intrusion detection/prevention, identity-based controls, secure internet browsing and traffic auditing are used to reduce unauthorised access and identify unusual patterns.
Data protection	Data classification, encryption in transit and at rest, data loss prevention, secure storage and controlled sharing protect school and student data.
Backup and recovery	Critical data is backed up regularly and stored securely. Disaster recovery and business continuity arrangements are maintained to reduce disruption following incidents.
Third-party security	External IT providers and learning applications are vetted for security, data protection, age-appropriateness, reliability and educational value.

Control Area	School Expectation
Audit and review	Filtering, monitoring, access, cybersecurity and online safety arrangements are reviewed through SLT, safeguarding, ICT and LAB oversight.

Safeguarding monitoring alerts, concerns or patterns are reported to the CPC/DSL. Technical security alerts are reported to the Digital Safety Officer / ICT Engineer and escalated to SLT. The school will balance student privacy with its duty to safeguard and protect the school community.

14. Data Protection and Confidentiality

- Personal data must be handled lawfully, fairly, securely and only for approved educational, safeguarding, administrative or legal purposes.
- Staff must not upload, email, message or share student data through unauthorised systems, personal accounts, personal devices or unapproved applications.
- Sensitive safeguarding information must be recorded and stored through Guard and shared only with authorised individuals on a need-to-know basis.
- Personal information may be shared with ADEK or authorised authorities where required by law, regulation or safeguarding procedures. Parents are informed of school obligations to share data with ADEK as required by ADEK policy.
- External providers must comply with data protection requirements and contracts must include appropriate confidentiality and data protection terms.
- Cybersecurity incidents, data breaches or suspected unauthorised access must be reported immediately to the ICT Engineer/Digital Safety Officer, Principal and, where safeguarding-related, the CPC/DSL.

15. Online Challenges, Cyberbullying and Child-on-Child Abuse

15.1 Online Challenges

Online challenges are activities or dares that children are encouraged to perform, record and share online. They may appear harmless but can create serious safeguarding, behavioural, wellbeing and legal concerns.

- Online challenges can normalise dangerous risk-taking behaviour, injury, humiliation, self-harm, illegal activity or harmful peer pressure.
- They can be linked to cyberbullying, coercion, fear of missing out, social validation and viral algorithms.
- Students must not encourage, perform, record or share dangerous or harmful online challenges.
- Concerns about online challenges must be reported to a trusted adult, the CPC/DSL or school leaders immediately.
- The school will respond through safeguarding, pastoral support, parent communication, behaviour procedures and external referral where necessary.

GEMS Winchester School, Abu Dhabi

Madinat Zayed

+971 (02) 403 5499

<http://gemswinchesterschool-abudhabi.com/>

WSA Investing In YOU!

15.2 Cyberbullying and Online Child-on-Child Abuse

- Cyberbullying includes repeated or serious online behaviour intended to harm, intimidate, embarrass, exclude or control another person.
- Online child-on-child abuse may include sexualised language, coercion, pressure to share images, non-consensual image sharing, harassment, impersonation, group exclusion, threats or harmful rumours.
- The school will treat cyberbullying and online child-on-child abuse as behaviour and safeguarding concerns, with support for those harmed and proportionate action for those responsible.
- Students are taught to save evidence safely, block/report users where appropriate, avoid retaliation and seek help promptly.

16. Youth-Produced Sexual Imagery and Illegal or Harmful Content

All incidents involving youth-produced sexual imagery, suspected sexual exploitation, grooming, non-consensual image sharing, sextortion or illegal imagery are safeguarding concerns and must be reported to the CPC/DSL immediately.

- Staff must not view, download, copy, print, forward, share or save sexual imagery or suspected illegal content.
- If content is accidentally viewed, staff must close or secure the device/screen, avoid further viewing, preserve the situation as safely as possible and report immediately to the CPC/DSL.
- Students must not be asked to forward content to staff. If evidence is required, the CPC/DSL and Principal will seek appropriate safeguarding, GEMS, ADEK, Police or external agency guidance.
- Parents will be engaged where appropriate and safe to do so, in line with safeguarding procedures and the best interests of the child.
- The school will provide support, risk assessment and referral for students who are harmed, coerced, exploited, responsible for sharing or otherwise involved.

17. Digital Incident Response

All digital incidents are recorded, investigated and acted upon proportionately. The school response will consider safeguarding risk, intent, harm, age, additional needs, repetition, legality, data risk, wider community impact and whether external reporting is required.

Category	Examples	Response
Level 1: Low-level or accidental breach	Examples: accidental access to non-harmful inappropriate material, first-time low-risk misuse, minor off-task use.	Education, reminder of expectations, teacher/pastoral follow-up, parent contact if needed, record locally if appropriate.
Level 2: Digital incident or repeated misuse	Examples: repeated misuse, VPN/proxy attempts, unauthorised recording,	Report to pastoral/SLT and ICT as required; parent contact; behaviour response;

GEMS Winchester School, Abu Dhabi

Madinat Zayed

+971 (02) 403 5499

<http://gemswinchesterschool-abudhabi.com/>

WSA Investing In YOU!

Category	Examples	Response
	inappropriate messaging, cyberbullying, online challenge concerns, bypassing teacher direction.	temporary removal of access or device privileges; record on school systems and Guard if safeguarding-related.
Level 3: Safeguarding concern or serious harm	Examples: grooming, exploitation, YPSI, threats, self-harm/suicide content, radicalisation/extremism, severe cyberbullying, discriminatory abuse, illegal content, coercion, child-on-child abuse.	Immediate report to CPC/DSL; record on Guard; support and risk assessment; Principal/CST involvement; ADEK, Police, FCA or other external referral where required; preserve evidence; do not investigate independently.
Level 4: Cybersecurity or data incident	Examples: malware, hacking, data breach, account compromise, ransomware, unauthorised access, serious system outage or security breach.	Report to ICT/Digital Safety Officer and Principal immediately; isolate systems; follow incident response and business continuity plan; notify GEMS and ADEK where required; communications only through authorised channels.

17.1 Reporting and Recording

- Any staff member who identifies or receives a digital safeguarding concern must report it to the CPC/DSL or Deputy CPC/DSL as quickly as possible and record it on Guard where appropriate.
- All high-risk concerns must be reported immediately to the CPC/DSL or Deputy CPC/DSL and escalated to the Principal.
- Technical incidents must be reported to the ICT Engineer / Digital Safety Officer immediately, with safeguarding concerns also reported to the CPC/DSL.
- Records must be factual, timely, signed/dated where required, and include the concern, actions taken, decisions, outcomes and referrals.
- The Principal will ensure digital incidents requiring ADEK audit evidence are documented, signed and stored in line with the ADEK School Records Policy.

17.2 Evidence and Investigation

- Students and staff should not delete relevant evidence unless directed by the CPC/DSL, Principal, Police or authorised authority.
- Evidence must not be shared beyond those who need to know. Screenshots or downloads of illegal or sexual imagery must not be taken by staff or students.
- Staff must not conduct their own safeguarding investigation. The CPC/DSL, Principal and external agencies will determine next steps.
- Where a personal device is involved, action will follow the BYOD Policy, Behaviour Policy, Safeguarding Policy, ADEK requirements and UAE law.

GEMS Winchester School, Abu Dhabi

Madinat Zayed

+971 (02) 403 5499

<http://gemswinchesterschool-abudhabi.com/>

WSA Investing In YOU!

17.3 Support and Sanctions

- Students affected by online harm will be listened to, supported and protected from further harm.
- The school may implement safety plans, restorative interventions, counselling/wellbeing support, risk assessments, parental engagement, schedule changes, supervision, loss of access, behaviour sanctions or external referrals.
- Responses will consider age, maturity, additional learning needs, intent, coercion, vulnerability, risk and the impact on the wider school community.
- Where misconduct by staff, volunteers, visitors or contractors is alleged, the school will follow allegations, HR, safeguarding and safer working practice procedures.

18. Distance Learning and Virtual Interactions

- Distance learning will use approved school platforms and safeguarding arrangements.
- Students and staff must follow the same standards of respectful conduct, privacy, safeguarding and academic honesty online as they do in school.
- Live sessions should be planned, professional and appropriately supervised. Recording of sessions is permitted only when authorised and in line with consent, privacy and safeguarding procedures.
- Virtual interactions with invited visitors must be risk assessed, have parental consent and, where required, ADEK approval in line with relevant policies.
- Students must not record, screenshot or share images, chat logs or videos from virtual lessons unless explicitly authorised by the teacher for learning purposes.

19. Monitoring, Audit and Review

The school will monitor the effectiveness of this policy through safeguarding, pastoral, curriculum, ICT, parent engagement and governance processes.

- The policy is reviewed annually by the Principal, CPC/DSL, Digital Safety Officer / ICT Engineer and LAB, and earlier when there are changes to ADEK requirements, GEMS policy, UAE law, technology risks, school systems or significant incidents.
- The CPC/DSL and Digital Safety Officer will review patterns in online safety concerns, filtering alerts, monitoring reports, Guard records, behaviour logs, parent/student feedback and training completion.
- The school will use student voice, staff feedback and parent engagement to strengthen online safety education and guidance.
- Policy updates will be communicated to students, parents, staff and visitors through appropriate channels. Student-friendly versions will be provided where appropriate.

20. Associated Policies and Documents

- GEMS Safeguarding / Student Protection Policy 2025-26
- GEMS Safer Working Practice Guidance and Staff Code of Conduct
- GEMS Guard safeguarding case-management procedures
- ADEK School Digital Policy
- ADEK School Safeguarding Policy
- ADEK School Student Protection Policy
- ADEK School Student Behaviour Policy and Parent Engagement Policy
- WSA BYOD Policy 2025
- WSA Behaviour Policy 2025-26
- WSA Anti-Bullying Policy 2025-26
- WSA Inclusion Policy
- WSA Learner Mental Health and Wellbeing Policy 2025-26
- WSA Educational Risk Policy
- WSA Parent Handbook
- Parents and Students Cybersecurity Guide
- Digital Device Responsible Use Agreement / Acceptable Use Agreements
- Data Protection, Records, Digital Media, Social Media and Cybersecurity procedures
- Extracurricular Activities and Events, Off-site Visits and Visitor procedures

Appendix A: Student Online Safety Code

This student-friendly code should be adapted for age and stage, including simplified versions for younger learners.

1. I use school technology for learning and follow teacher instructions.
2. I keep passwords private and log out when I finish.
3. I do not use VPNs, hotspots or tricks to bypass school safety systems.
4. I am kind and respectful online, even when I disagree.
5. I do not search for, create, save or share harmful, violent, sexual, bullying, discriminatory or illegal content.
6. I do not take or share photos, videos or recordings of others without permission.
7. I check before I click, download, buy, sign up or share personal information.
8. I know that not everything online is true and I check information carefully.
9. I use AI only when my teacher allows it and I do not use it to cheat, bully, copy or create harmful content.
10. I tell a trusted adult if anything online worries me, upsets me, pressures me or makes me feel unsafe.

Appendix B: Family Conversation Starters

Theme	Conversation starter
Content	What have you seen online recently that made you curious, uncomfortable or unsure? What would you do if something upsetting appeared?
Contact	What would you do if someone you do not know messaged you, asked for a photo, offered a gift or wanted to meet?
Conduct	How can we show kindness and respect online, especially when we disagree? What should we never share about ourselves or others?
Commerce	Have you ever been asked to buy something, click a link, enter personal details or join a competition online? How can we check if it is real?
AI	How can we tell whether AI information is accurate? What information should we never put into AI tools?
Help-seeking	Who are your trusted adults at home and school? What would help you tell us quickly if something went wrong online?

Appendix C: Online Safety Incident Response Flow

1. Concern identified or disclosed: student, staff, parent, monitoring alert, report, platform notification or external agency information.
2. Immediate safety: ensure the student is safe; take emergency action if there is imminent risk of harm.

3. Report: inform the CPC/DSL or Deputy CPC/DSL immediately for safeguarding concerns; inform ICT/Digital Safety Officer for technical or cyber incidents.
4. Record: enter safeguarding concerns on Guard without undue delay; record technical incidents in the appropriate ICT/cybersecurity log.
5. Preserve evidence safely: do not forward, download, print or screenshot illegal or sexual imagery; follow CPC/DSL and external agency advice.
6. Triage: determine Level 1, 2, 3 or 4 response, considering harm, legality, age, vulnerability, intent, repetition and data/cyber risk.
7. Support and action: provide pastoral/safeguarding support, parent engagement, sanctions where appropriate, technical containment, risk assessment and safety planning.
8. Escalate: refer to GEMS Central Safeguarding Team, ADEK, Police, Family Care Authority or other authorities where required.
9. Review: document outcomes, monitor recurrence, update lessons learned, review filters/controls and communicate learning to relevant stakeholders.

Appendix D: Staff Quick-Reference - Do and Do Not

Action	Expectation
Do	Report online safety and safeguarding concerns promptly to the CPC/DSL and record on Guard where appropriate.
Do	Use official school systems for teaching, communication and storage.
Do	Challenge and report attempts to bypass filtering, inappropriate searches, harmful content, cyberbullying or online challenges.
Do	Preserve evidence safely and seek advice when illegal or sexual content may be involved.
Do not	Use personal social media, personal email or private messaging apps to communicate with current students.
Do not	View, save, forward, print, screenshot or share illegal or suspected illegal sexual imagery.
Do not	Take photos of student injuries for safeguarding evidence.
Do not	Investigate safeguarding concerns independently or promise confidentiality to students.
Do not	Upload student data to unapproved external applications, AI tools or personal accounts.

Appendix E: Alignment Checklist

Requirement / source area	Where addressed in this policy
ADEK School Digital Policy - responsible usage policies for students, parents, staff and visitors	Sections 3, 8, 10, Appendix A, Appendix D
ADEK School Digital Policy - online risks: harmful content, unsafe interaction, harmful conduct, scams/finance risks	Section 7 and curriculum requirements in Section 9
ADEK School Digital Policy - restrict VPNs unless explicitly authorised	Sections 10.2 and 10.3
ADEK School Digital Policy - staff personal social media and personal email restrictions	Sections 12.1 and 12.4
ADEK School Digital Policy - data/cybersecurity, filtering, monitoring, incident response and data protection	Sections 13, 14 and 17
ADEK School Digital Policy - digital media consent and publication requirements	Section 12.2
ADEK School Safeguarding Policy - duty of care, safeguarding awareness and vigilance in online spaces	Sections 1, 6, 8, 9 and 19
ADEK Student Protection Policy - best interests, zero tolerance, reporting and student voice	Sections 6, 8, 17 and 19
GEMS Safeguarding / Student Protection Policy - online safety policy, 4Cs, filtering/monitoring, AI, image-sharing, cyberbullying and mobile/smart technology	Sections 7, 10, 11, 12, 13, 15, 16 and 17
GEMS Safeguarding / Student Protection Policy - Guard recording and CPC/DSL oversight	Sections 8.3, 16, 17 and Appendix C
WSA BYOD Policy 2025 - personal devices, no social media/VPN, no unauthorised recording, device privileges	Section 10.3
WSA cybersecurity guidance - parents educate, protect, monitor and support students	Sections 9.3 and Appendix B