

CYBER SECURITY AND ONLINE SAFETY POLICY

PURPOSE

The purpose of this Cyber Security and Online Safety Policy is to protect the school's digital information, systems, and users from cyber threats, and to ensure a safe, secure, and responsible digital learning environment. It also guides students in developing positive digital habits that protect their wellbeing and reflect the school's values of kindness, respect, and responsibility.

SCOPE

This policy applies to all students, teachers, administrative staff, and visitors who access or use the school's IT resources, including school computers, networks, email accounts, and internet services. It extends to both on-site and remote access of school systems, as well as the use of personal devices on the school network.

ROLES AND RESPONSIBILITIES

Stakeholder	Responsibilities
Principal & SLT	- Ensure this policy is implemented, reviewed annually, and communicated to all staff, students, and parents. - Ensure an appropriate member of staff is designated as Online Safety Lead. - Ensure all staff receive annual training on cyber security, online safety, and the school's Acceptable Use Policy. - Ensure KHDA and UAE legal requirements relating to data protection and online safety are met.
IT Coordinator / Online Safety Lead	- Maintain and update the school's IT systems, including firewalls, content filters, and security patches. - Maintain an incident log and review it termly to identify trends and strengthen safeguards. - Ensure all software and applications used by the school are approved and appropriately licensed. - Deliver staff and student digital literacy training aligned with this policy.
Teaching Staff	- Model responsible digital behaviour and professional communication at all times. - Supervise students' online activity during lessons and ensure usage is purposeful and age-appropriate. - Report any cyber security incidents or safeguarding concerns related to online activity to the IT Coordinator and DSL immediately.
Students	- Use school devices and internet access only for educational purposes. - Keep usernames and passwords confidential and never share login details. - Report any concerning online activity, including cyberbullying, phishing, or inappropriate content, to a trusted adult. - Behave responsibly and respectfully in all digital communications.
Parents and Guardians	- Support the school's online safety expectations at home. - Model responsible social media and digital behaviour. - Alert the school if their child discloses any online safety concerns. - Images or Videos taken at a school event e.g Sports Day that contain other students should not be shared on social media without consent

ACCEPTABLE USE

- School devices and internet should be used primarily for educational purposes.
- Users must not use school resources for illegal, harmful, or unethical activities.
- Accessing inappropriate or offensive content is strictly prohibited.
- Staff must ensure that students' online learning is supervised, age-appropriate, and purposeful, especially in EYFS and Primary where children are more vulnerable.
- Use of personal devices for schoolwork must comply with the same expectations of professionalism and safety.

PASSWORDS AND USER ACCOUNTS

- All users must keep their usernames and passwords confidential.
- Passwords should be strong (minimum 8 characters, including numbers and symbols).
- Do not share login details with anyone.
- Students in Primary and Secondary will receive age-appropriate guidance on creating and managing secure passwords.

DATA PROTECTION

Personal information of students and staff must be handled carefully, stored securely, and shared only in compliance with UAE Federal Law No. 45 of 2021 on Personal Data Protection.

- Do not share sensitive data (such as student records) without proper authorisation.
- Always log off or lock your computer when leaving it unattended.
- Data sharing with third parties must comply with UAE data protection regulations and only be done with parental consent where appropriate.

DATA CLASSIFICATION

All school data is classified as either Public, Internal, Confidential, or Restricted. Staff must only access and share data at the appropriate classification level. Student records, medical information, and safeguarding documentation are classified as Restricted and must never be shared outside authorised channels.

SOFTWARE AND DOWNLOADS

- Only approved software may be installed on school devices.
- Do not download files or applications from untrusted sources.
- The IT team will regularly review and update approved software lists and ensure licences are valid.

ARTIFICIAL INTELLIGENCE AND GENERATIVE TOOLS

The use of artificial intelligence (AI) tools, including generative AI platforms, must align with the school's academic integrity policy. Students may not use AI tools to generate work submitted for assessment unless explicitly permitted by the teacher for a specific task. Staff must assess student submissions for authenticity in accordance with the school's assessment policy. The school's IT Coordinator maintains an approved list of AI and digital tools that may be used within the school environment.

EMAIL AND COMMUNICATION

- Use respectful and professional language in all communications.
- Be cautious with email attachments and links to avoid phishing scams.
- Report any suspicious emails to IT staff immediately.
- Staff should model responsible communication for students and ensure that online platforms used for learning are secure and moderated.

Device Use

- Students and staff must care for school-owned devices.
- Personal devices connected to the school network must follow the same security guidelines.
- All devices must be password-protected and kept updated with the latest security patches.

REPORTING INCIDENTS

Report any cyber security incidents (e.g. data breaches, malware, ransomware, or suspicious activity) to the IT Coordinator immediately. A log of incidents will be maintained and reviewed termly.

Incident Type	Initial Response Target
Suspected data breach (student or staff data)	Report to Principal and IT Coordinator within 1 hour of discovery
Cyberbullying or online harm involving a student	Report to DSL within 1 hour; parent contact within 24 hours
Malware or ransomware detected on school network	Isolate affected device immediately; IT Coordinator to assess within 2 hours
Phishing email targeted at staff or students	Report to IT Coordinator immediately; school-wide alert if widespread
Inappropriate content accessed by a student	Report to class teacher and IT Coordinator; DSL if safeguarding concern

CONSEQUENCES

Failure to comply with this policy may result in disciplinary action, loss of access to IT resources, and, if necessary, legal action under UAE Federal Decree Law No. 34 of 2021 on Cybercrime. Students will also be supported through digital citizenship education to prevent repeat behaviours.

PREVENTING CYBER ADDICTION

AESD is committed to protecting students from overreliance on technology and the risks of cyber addiction. Technology in the school is used sparingly and only when it adds educational value. Teachers carefully plan its use to ensure that learning remains purposeful, interactive, and balanced. Younger students, particularly in EYFS and Primary, are encouraged to develop social, physical, and creative skills without excessive screen exposure. The school also works in partnership with parents to promote healthy digital habits at home.

SOCIAL MEDIA CONDUCT

AESD recognises that negative or defamatory use of social media can harm individuals and the reputation of the school community. Staff and students are educated about respectful digital behaviour, the legal consequences of online defamation under UAE law, and the importance of safeguarding the school's reputation and community. Any incidents of online defamation or harassment will be addressed promptly through disciplinary procedures, parental involvement, and, where necessary, escalation to local authorities in line with UAE cybercrime laws.

MONITORING AND REVIEW

The IT Coordinator reviews the incident log termly. The Online Safety Lead conducts an annual audit of filtering, monitoring, and content controls. This policy is reviewed annually in August and updated following any significant incident or change to KHDA requirements or UAE law.

Authorised by: Principal

Review date: August 2027