Cyber Bullying Policy

Version	Document Title	Author	Date Created	SLT Approved	Principal Approved	Review Date
0.1	Cyber Bullying Policy	IT	August 2024	August 2025	August 2025	August 2026

CONTENTS

Purpose
The purpose of this Cyber Security Policy is to protect the school's digital information, systems, and users from cyber threats and ensure a safe, secure, and responsible digital learning environment. It also ensures that students are guided to develop 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.

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 & 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 and stored securely.
- Do not share sensitive data (such as student records) without proper authorization.
- 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.

Software & 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 licenses are valid.

Email & 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 the 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, or suspicious activity) to the IT Coordinator immediately.
- A log of incidents will be maintained and reviewed termly to identify trends and strengthen safeguards.

Consequences
Failure to comply with this policy may result in disciplinary action, loss of access to IT resources, and, if necessary, legal action. 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.

Preventing and Addressing Social Media Defamation

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