E-safety Policy

POLICY FOR	E-Safety
PERSON RESPONSIBLE	Head of Pastoral/Digital Leader
REVIEW DATE	June 2026
REVIEWED BY	Assistant Principals and Head of School
APPROVED DATE	June 2026
APPROVED BY	Executive Principal
DATE OF NEXT REVIEW	June 2027
RELATED POLICIES	Rewards and Sanctions Policy, Safeguarding Policy, Online Security Policy, Anti- bullying Policy, Acceptable use of digital resources Policy, Wellbeing Policy

Executive Principal / CEO .....

E-Safety Policy

Introduction:

The Westminster School, Dubai (TWS) is committed to providing an exceptional education for young people. The safety and welfare of our students is of utmost importance. Ensuring that students can safely access new technology and learn how to participate in the digital world without compromising their safety and security is a key part of delivering a well-rounded programme of education.

E-Safety at a simple level means being safe on the internet. Some people also include the safe use of technology in this as well. The pace at which technology is evolving can make it difficult to know what to include when talking about the safe use of the internet.

Background / Rationale:

New technologies have become integral to the lives of young people in today's society, both within schools and in their lives outside school.

The Internet and other digital and information technologies are powerful tools, which open new opportunities for everyone. Electronic communication helps teachers and students learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning.

Information and Communications Technology (ICT) covers a wide range of resources including web-based and mobile learning. It is also important to recognise the constant and fast-paced evolution of ICT within our society as a whole. Currently the internet technologies used by students and staff both inside and outside of the classroom include:

- Websites
- AI Tools
- Learning Platforms and Virtual Learning Environments
- Cloud-based services and storage
- Video conferencing tools
- Collaborative tools - Google Docs, Padlet, Canva, Miro, Microsoft Teams collaboration
- Digital content creation tools - AI image generators, video editors, design tools
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs
- Podcasting
- Video Broadcasting / Vlogs
- Downloading
- Gaming on multiple platforms

- Mobile/Smart phones with text, video and/or web functionality
- Wearable devices including smart watches, fitness trackers, and other internet-enabled technology
- Other mobile devices with web functionality

There is a need to provide safe internet and related communications for all the students and staff.

Purpose:

This E-Safety policy enables our school to create a safe e-learning environment that:

- Protects students from harm.
- Provides guidance to staff while contacting parents and students.
- Provides guidance to staff and students towards safe use of internet.
- Provides clear expectations for all on acceptable use of the internet.

Aims of the e-safety policy:

- Protecting and educating students and staff in their use of technology.
- Informing teachers and parents/guardians about their role in safeguarding and protecting students at school and home.
- Implementing policies and procedures in place to help prevent incidents of cyber-bullying within the school community.
- Having effective and clear measures to deal with and monitor cases of cyber-bullying.

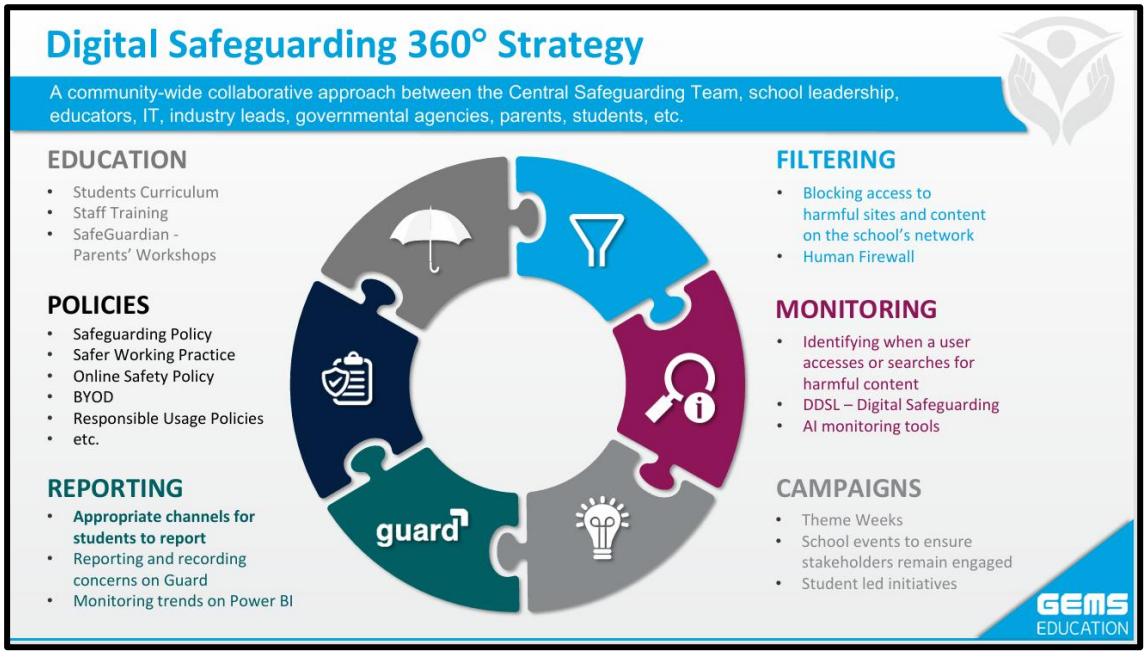
E-Safety education is provided in the following ways:

- Key e-safety messages should be reinforced as part of a planned programme of assemblies/activities.
- Students should be taught in all lessons to be critically aware of the materials / content they access on-line and are guided to validate the accuracy of information.
- Students should be helped to understand the need to adopt safe and responsible use of ICT, the Internet and mobile devices both within and outside school.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.
- Rules for use of ICT systems / Internet are posted in the students' planner.
- Students should be educated about the ethical and responsible use of Artificial Intelligence (AI), including understanding AI-generated content, safeguarding personal data when interacting with AI tools, and being aware of potential biases, misinformation, and overreliance on AI-driven platforms.

Threats of using digital technology

- Access to illegal, harmful or inappropriate images or other content
- Unauthorized access to, loss of, and sharing of personal information

- Internet grooming
- Radicalisation - The risk of students being exposed to or influenced by extremist or harmful ideologies through online content, social media, or inappropriate online contacts.
- The sharing and distribution of personal images without consent
- Inappropriate communication and contact with others
- Cyber-bullying
- Access to unsuitable video and internet games
- An inability to evaluate the quality, accuracy/reliability and relevance of information on the internet
- Plagiarism and copyright infringement
- Downloading illegal or offensive content or applications
- Excessive use which may impact social and emotional development and Learning addiction
- Misuse of Artificial Intelligence (AI): The increasing use of AI tools can lead to threats such as the spread of misinformation through deepfakes or AI-generated fake content, privacy violations from data misuse, overdependence on AI for decision-making, and exposure to biased or unethical algorithms.



Filtering and Monitoring

The school is committed to ensuring a safe and secure digital environment for all students and staff through appropriate filtering and monitoring systems.

Filtering

The school uses web-filtering and network security systems to restrict access to inappropriate, harmful, illegal, or unsafe online content, including:

- Adult or violent material

- Extremist or harmful content
- Gambling and illegal websites
- Malware, phishing, and unsafe downloads
- Websites or applications that may pose safeguarding risks
  Filtering levels are age-appropriate and regularly reviewed by the IT team and school leadership.

Monitoring

The school monitors the use of school devices, accounts, networks, and online platforms to safeguard students and protect school systems. Monitoring may include internet usage, search activity, emails, and online communications. Any concerns related to cyberbullying, safeguarding, inappropriate behavior, or attempts to bypass security systems will be investigated and managed in line with the school's safeguarding and behavior policies.

Responsibilities

- The ICT Engineer maintains filtering and monitoring systems.
- Staff supervise and promote safe online behavior.
- Students are expected to use technology responsibly and follow the Acceptable Use Policy.

The school regularly reviews its filtering and monitoring procedures to respond to emerging online safety risks and technologies.

ROLES AND RESPONSIBILITIES

Roles & and responsibility of ICT Engineer and Digital DDSL

- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provides training and advice for staff.
- Liaises with the KHDA / relevant body if needed.
- Liaises with school technical staff when needed.
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
- Reports regularly to Senior Leadership Team.

Guidelines for students and staff

- All staff should be trained in e-safety issues and be aware of the potential for serious child protection / safeguarding issues which arise from:
  - Sharing of personal data
  - Access to illegal / inappropriate materials
  - Inappropriate on-line contact with adults / strangers
  - Potential or actual incidents of grooming

- Cyber-bullying

- Students must report any suspected misuse or problem to the Head of House/Head of Pastoral for investigation / action / sanction.
- All digital communication with students / parents / carers should be on a professional level and only carried out using official school systems.
- E-safety guidelines are embedded in all aspects of the curriculum and other activities.
- Students understand and follow the e-safety and Digital Use Acceptable Policy.
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Staff oversee the usage of digital technologies, including smart devices and cameras, during lessons and other school activities (where permissible), ensuring compliance with existing policies concerning these devices.
- In lessons where internet use is pre-planned, students should be guided to the sites checked as suitable for their use, and those processes are in place for dealing with any unsuitable material found in internet searches.
- Students and staff must use AI tools responsibly, ensuring ethical use, data privacy, and verifying information accuracy at all times.

Note: The student to avoid sharing the school account credentials with others.

Rules for publishing material online (including images of students):

School websites are a valuable tool for sharing information and promoting students' achievements. We recognise the potential for abuse. Therefore, the following principles will always be considered:

- Staff must not take photographs of students using their personal devices.
- All student photographs must be taken using TWS device.
- Only images of students in suitable dress should be used and group photographs are preferred (though not exclusively) in preference to individual photographs.
- Parents are given the opportunity to withdraw permission for the school to publish images/audio/video of their child on the school website/publications.
- Content should not infringe the intellectual property rights of others – copyright may apply to text, images, music or video that originate from other sources.
- All copied or embedded content should be properly referenced.
- Content should be polite and respect others.
- Published content should be proofread by a member of the school's Senior Leadership Team before being published.
- Parent consent must be taken before publishing images/audios/videos of their child.

Student rules for acceptable internet use:

We will adopt the rules as laid out below in an age-appropriate way for the students at TWS.

- I will ask permission from an adult before using the Internet.
- I will use computers and tablets safely.
- I will not look for websites that I know I'm not allowed to see.
- If I see anything that I know is wrong, I will tell an adult straight away.
- I will not download anything without permission from an adult.
- I will not use memory sticks on school computers without permission from an adult.
- I will ask an adult before sending emails to unknown people.
- I will be polite and respect others when using the Internet.
- I will not give out any personal information over the Internet.
- I will not share my login details with others.
- I understand that the school may check my computer files and check what I am doing.
- I may/may not be allowed to play games on the computer to enhance my educational knowledge
- I will use GEMS official id to communicate with school staff.
- I understand that failing to adhere to E Safety policy and TWS Acceptable Use Digital Policy might lead to strict disciplinary action against me according to the school's Rewards and Sanctions Policy.

Visitors' rules for acceptable internet use:

Visitors' Internet use will vary depending upon the purpose of their visit. Generally, we expect all visitors to abide by the following rules:

- I will respect the facilities by using them safely and appropriately.
- I will not use the Internet for personal financial gain, political purposes, advertising, personal or private business.
- I will not deliberately seek out inappropriate websites.
- I will report any unpleasant or upsetting material to a member of staff immediately.
- I will not download or install program files.
- I will not use USB memory devices on school computers.
- I will be polite and respect others when communicating over the Internet.
- I will not share my login details.
- I will not carry out personal or unnecessary printing.
- I understand that the school may check my computer files and monitor my Internet use.

Students:

Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

- Students will be expected to know and understand policies on the use of mobile devices and digital cameras.
- Students should also know and understand policies on the taking / use of images and on cyber-bullying.
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realize that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.

Parent:

Parents and caregivers are encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events
- Access to parents' sections of the website / blog
- Their children's personal devices in the school (where this is allowed)
- The school will monitor the impact of the policy using:
  - Logs of reported incidents
  - Surveys of reported incidents: ➢ Students ➢ Parents / Caregivers ➢ Staff

Confidentiality:

All reported cases will be treated with utmost confidentiality at all times.

Referral:

The school may refer the student to a government or non-government agency concerned if deemed necessary.

Monitoring and Evaluation:

The Pastoral Team and the IT team will monitor and evaluate the effectiveness of E-safety Policy alongside Rewards and Sanctions Policy annually. In case of new legislation from UAE government and United Nation pertaining to Bullying and or Cyber Bullying, the policy should be amended in accordance with the national and international law set forth.