E-safety Policy

Introduction

Deira Private School, Dubai (DePS) is committed to providing an exceptional education for young people. The safety and welfare of our students are 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 basic level, means being safe on the internet. Some people also include the safe use of technology in this definition. The pace at which technology is evolving can make it difficult to know what to include when discussing the safe use of the internet.

Background / Rationale

Integration of Technology

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

Opportunities and Tools

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

Scope of ICT

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

Websites

- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Social Networking
- Downloading
- Gamification and AFL tools
- Mobile/Smart phones with text, video, and/or web functionality
- Other mobile devices with web functionality
- There is a need to provide safe internet and related communications for all 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 when contacting parents and students.
- Provides guidance to staff and students on the safe use of the internet.
- Establishes clear expectations for acceptable internet use.
- 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 to help prevent incidents of cyberbullying within the school community.
- Having effective and clear measures to address and monitor cases of cyberbullying.
- E-Safety Education
- Educational Strategies

E-Safety education is provided in the following ways:

- Key e-safety messages should be reinforced as part of a planned programme of assemblies and activities.
- Students should be taught in all lessons to be critically aware of the materials and content they access online and be guided to validate the accuracy of information.
- Students should 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.

Threats of Using Digital Technology

Types of Threats

The following are key threats associated with digital technology:

- Access to illegal, harmful, or inappropriate images or other content
- Unauthorized access to, loss of, and sharing of personal information
- Internet grooming
- Radicalization
- Sharing and distribution of personal images without consent
- Inappropriate communication and contact with others

Cyberbullying

- Access to unsuitable video and internet games
- 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 lead to addiction

Roles and Responsibilities

E-Safety Officer (DSL)

- Leads the e-safety committee.
- Takes day-to-day responsibility for e-safety issues and plays a leading role in establishing and reviewing the school e-safety policies and documents.
- Ensures that all staff are aware of the procedures to follow in the event of an e-safety incident.
- Provides training and advice for staff.
- Liaises with KHDA/relevant bodies as needed.
- Liaises with school technical staff as needed.
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
- Meets regularly with the E-Safety Governor to discuss current issues, review incident logs, and filtering/change control logs.

- Attends relevant meetings/committees of Governors.
- Reports regularly to the Senior Leadership Team.

Guidelines for Students and Staff

Staff Responsibilities

All staff should be trained in e-safety issues and be aware of potential serious child protection/safeguarding issues arising from:

- Sharing of personal data
- Access to illegal/inappropriate materials
- Inappropriate online contact with adults/strangers
- Potential or actual incidents of grooming

Cyberbullying

Student Responsibilities

Students must report any suspected misuse or problems to the Head of House/Head of Pastoral for investigation/action/sanction.

- All digital communication with students/parents/carers should be professional and conducted 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 use of digital technologies, including smart devices and cameras, during lessons and other school activities (where permissible), ensuring compliance with existing policies concerning these devices.

Pre-Planned Internet Use:

In lessons where internet use is pre-planned, students should be guided to sites checked as suitable for their use, and processes should be in place for dealing with any unsuitable material found in internet searches.

Note: Students should avoid sharing their school account credentials with others.

Rules for Publishing Material Online

Principles for Publishing

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

- Staff must not take photographs of students using personal devices.
- All student photographs must be taken using DePS devices.
- Only images of students in suitable dress should be used, and group photographs are preferred (though not exclusively) over 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 on 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 respectful.
- Published content should be proofread by a member of the school's Senior Leadership Team before being published.
- Parent consent must be obtained before publishing images/audio/videos of their child.

Student Rules for Acceptable Internet Use

We will adopt the rules outlined below in an age-appropriate manner for the students at DePS:

- 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 immediately.
- I will not download anything without permission from an adult.
- I will ask an adult before sending emails to unknown people.
- I will be polite and respectful 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 monitor my activities.
- I may or may not be allowed to play games on the computer to enhance my educational knowledge.
- I will use my school ID to communicate with school staff.

- I understand that failing to adhere to the E-Safety Policy and DePS Acceptable Use Digital Policy might lead to strict disciplinary action according to the school's Rewards and Sanctions Policy.

Visitor Rules for Acceptable Internet Use

Visitor internet use will vary depending on 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, or personal/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 respectful 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.

Monitoring and Evaluation

- Impact Monitoring
- The school will monitor the impact of the policy using:
- Logs of reported incidents
- Regular reviews of filtering and monitoring reports

Feedback from staff, students, and parents

Annual Review

The Pastoral Team and the IT team will monitor and evaluate the effectiveness of the E-Safety Policy alongside the Rewards and Sanctions Policy annually. In case of new legislation from the UAE government or the United Nations pertaining to Bullying and/or Cyberbullying, the policy will be amended in accordance with national and international laws.

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.

Document	E Safety Policy
Date written	April 2010
Last reviewed	May 2025
Next Review	August 2026
Version	Working document