ENGLISH INTERNATIONAL SCHOOL OF TUNIS

British Curriculum

E-Safety Policy

.

Edited by	Software Engineer in charge of Network & IT	Imen Ben Abderrahmen	February 2025
Edited by	ICT & Computer Science Teacher	Oumaima Naceur	
Reviewed by	Interim Principal	Jacqueline Johnson	

Introduction

At English International School of Tunis (EIST), we believe that ICT (Information and Communications Technology) is central to all aspects of learning for both adults and children within the school and the wider community. ICT is a crucial resource for supporting teaching and learning while also playing a significant role in the everyday lives of children, young people, and adults.

Our aim is to empower young people with the skills they need to thrive in a digital world, equipping them for lifelong learning and future employment. We ensure that all students, regardless of their needs, have access to a range of up-to-date technologies in classrooms and ICT suites. ICT should be integrated into all learning experiences as a fundamental life skill rather than taught in isolation.
Given the constant evolution of digital technologies, students encounter a wide array of internet resources both within and outside the classroom. These include:

- Websites
- Learning platforms and virtual environments
- Email and instant messaging
- Social networking and chat platforms
- Blogs, podcasts, and video broadcasting
- Music streaming and downloading
- Gaming
- Mobile and smart devices

All users need to be aware of the range of risks associated with the use of these Internet technologies.

At EIST we understand the responsibility to educate our pupils on e-safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

We have signed up to and follow all educational programmes from Common Sense Media both as a teaching tool and a resource for teachers and parents. E-safety and responsible digital citizenship form a core part of our PSHE policy.

This e-safety policy reflects the need to raise awareness of the safety issues associated with information systems and electronic communication as a whole.

Whole school approach

E-safety is a shared responsibility across the entire school community. All staff members are expected to model and promote safe digital behaviors and adhere to the school's e-safety procedures.

Key areas of focus include:

- Safe use of email and internet resources
- Responsible use of school networks, equipment, and data
- Proper handling of digital images and technologies such as cameras and mobile devices
- Ensuring pupil information is published responsibly on the school website or social media
- Embedding e-safety education in classroom teaching

Staff are reminded/updated about e-safety regularly and new staff and students receive information on the school's acceptable use policy as part of their induction.

E-Safety in the Curriculum

E-safety education is integrated into the ICT and PSHE curricula. We strive to:

- Provide pupils with meaningful, ongoing guidance on e-safety.
- Educate pupils on the risks associated with social media and digital platforms.
- Teach pupils about respecting copyright and intellectual property.
- Raise awareness about online bullying (cyberbullying) and provide strategies for seeking help.
- Equip pupils with the skills to critically evaluate online content and conduct responsible searches.

Managing Internet Access

To ensure a safe and secure digital environment for all users, managing internet access is a critical component of our e-safety policy, with guidelines in place to minimize risks and promote responsible usage.

- Staff must preview any recommended sites before use. Particular care must be taken when using search engines with the children as these can return undesirable links.
- Raw image searches are discouraged when working with pupils.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents need to be advised to supervise any further research.
- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to an ICT leader, technician or member of SLT.
- It is the responsibility of the school, by delegation to the network manager, to ensure that antivirus protection is installed and kept up-to-date on all school machines.

Firewall Implementation

The school operates a single, independent network connected through a unified fiber-optic infrastructure, ensuring consistent connectivity and performance across all floors.
To safeguard this network, the school has implemented the **FortiGate** firewall, which ensures robust network security across the entire infrastructure.

Key Features Relevant to E-Safety

- **Content Filtering**: FortiGate provides web filtering to block access to inappropriate or harmful content, ensuring a safe online environment for pupils and staff.

- **Intrusion Prevention**: Advanced intrusion detection and prevention systems protect against unauthorized access and potential cyber threats.

- **Monitoring and Logging**: The firewall supports detailed logging of internet activity, enabling the school to monitor network usage and investigate any breaches of e-safety protocols.

- **Data Protection**: Encryption of data in transit ensures the security of sensitive information shared over the network.

By maintaining a consistent and secure firewall policy, the school reinforces its commitment to providing a safe digital environment for all users in line with the e-safety policy.

E-mail

Email is an essential communication tool for staff within the school and offers valuable educational opportunities. While email should not be considered private, it provides significant benefits, including:

- Direct written communication for staff and pupil-based projects within the school.
- Collaboration between schools, both locally and internationally.
- Opportunities for pupils to learn and practice age-appropriate email writing skills.

Publishing pupil's images and work

On a pupil's entry to the school, all parents/guardians are asked to give permission for their child's photo to be taken and to use their child's work/photos in the following ways:

- on the school website
- on social media
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, i.e. exhibition promoting the school
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically.)

Pupils' names will not be published alongside their image and vice versa without permission from the parents. Full names will not be published.

Social networking and personal publishing

Social networking and personal publishing present opportunities for creativity and connection but also come with risks. To ensure safe and responsible use, we:

- Advise pupils to avoid sharing personal information online that could reveal their identity or location.
- Educate pupils on the potential dangers of interacting with strangers on social media platforms.

Data protection

Personal data is recorded, processed, and transferred in line with local data protection regulations. Staff may only access school data on authorized devices and are prohibited from using personal devices for this purpose.

Responding to e-safety incidents/complaints

As a school we will take all reasonable precautions to ensure e-safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. The school cannot accept liability for material accessed, or any consequences of Internet access. Complaints relating to e-safety should be made to a member of the senior leadership team. Any complaint about staff misuse must be referred to the Head teacher.

- All users are aware of the procedures for reporting accidental access to inappropriate materials. Any breach must be immediately reported.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged and, depending on the seriousness of the offence; investigation by the Principal, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences
- Pupils and parents will be informed of the complaints procedure.

- Parents and pupils will need to work in partnership with staff to resolve issues.

Cyberbullying

Cyberbullying is the use of ICT, particularly mobile phones and the internet, to deliberately upset someone else. The whole school community has a duty to protect all its members and provide a safe, healthy environment.

It is important that we work in partnership with pupils and parents to educate them about Cyberbullying as part of our e-safety curriculum.

Prevention measures include:

- understand how to use these technologies safely and know about the risks and consequences of misusing them
- know what to do if they or someone they know are being cyber bullied.
- report any problems with Cyberbullying. If they do have a problem, they can talk to the school, parents, the police, the mobile network (for phone) or the Internet Service Provider (ISP) to do something about it.

www.kidscape.org and www.wiredsafety.org

Supporting the person being bullied

Support shall be given in line with the behaviour policy:

- Give reassurance that the person has done the right thing by telling someone and inform parents.
- Make sure the person knows not to retaliate or return the message.
- Help the person keep relevant evidence for any investigation (taking screen capture shots, not deleting messages.)
- Check the person knows how to prevent it from happening again e.g. blocking contacts, changing contact details.

- Take action to contain the incident when content has been circulated: remove content, contact the host (social networking site) to get the content taken down, use disciplinary powers to confiscate phones that are being used to cyber bully – ask the pupil who they have sent messages to.

Last reviewed: February 2025

Reviewed termly as things change rapidly