



Digital/cyber safety policy

Scope of the Policy

This policy applies to all members of the school (including staff, students, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the school.

Introduction

The goal of Our Own English High School, Al Ain (OOL) is to provide a 21st-century learning environment where all students have equitable access to technology and may develop into self-directed learners, collaborative team players, and both creators and consumers of knowledge. The goal of OOL's usage of digital technology in teaching and learning is to enhance student learning by utilizing both in-house resources and efficiently accessible internet resources. Students who behave responsibly and maturely when using the internet are entitled to it.

As part of their educational experience, students at Our Own English High School have safe and secure access to the Internet. Online safety is always a top priority, and OOL Teachers prepare for the creative application of technology to deliver excellent teaching and learning experiences for their students. All members of our OOL community, including parents and non-teaching staff, will benefit from our support of a best practice approach and safer working practices when we take a whole school approach to internet safety through common policies, guidance, continuous training, and professional development opportunities.

Roles and Responsibilities

- The Principal, SLT and the Digital Team are responsible for ensuring that the policy is implemented fully and reviewed regularly.
- The Principal, SLT and the Digital Team are responsible for ensuring that online safety is embedded within the curriculum and that teachers are confident in delivering high quality lessons that are age appropriate and show progression, building on prior learning.
- Staff have a particular responsibility to supervise use, plan access and set good examples. (In line with GEMS Acceptable Use Policy)
- At OOL we believe that online safety is everyone's responsibility.

A vast range of resources are covered by information and communications technology, including mobile and web-based learning. It's also critical to acknowledge how quickly and continuously ICT is evolving inside our society. Children are now utilizing the following internet technologies both within and outside of the classroom:

- Websites
- Phoenix Classroom (Learning Platforms and Virtual Learning Environments)
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Downloading from the internet
- Gaming
- Mobile/Smart phones with text, video and/or web functionality
- Other devices with web functionality.

OOL believes that the enormous benefits of technology and the IT network as a resource for education greatly exceed any possible drawbacks. Utilizing both current and upcoming technologies, we will equip our students with the skills they need to succeed in the competitive global electronic age and learn how to live in the twenty-first century. At OOL, we believe that every student's education must include access to the tools and resources of a global network as well as knowledge on when and how to use these technologies in an acceptable and productive manner.

Our Own English High School, Al Ain ensures that:

- We provide a systematically filtered internet service for everyone.
- We provide supervision and direction in Internet activities.
- Adopt programs that promote safe and ethical behaviours about digital rights and privacy information.
- Reinforce the importance of safe, disciplined, ethical, responsible, and respectful use of the Internet in all curriculum areas.
- We provide a digital learning curriculum that covers all areas of online safety at an age-appropriate level.
- Without endangering their safety and security, children can learn how to engage in the digital world and safely use new technologies.
- Teachers orient students in safe digital usages.
- When using anything they have accessed online, students are taught to respect copyright and provide credit to the original source of the information.
- Every employee and student are aware of the significance of password security and the necessity of logging out of accounts.
- When it comes to using ICT, the Internet, and mobile devices, staff members set a positive example.

- It features well-defined and comprehended protocols for safeguarding, preserving, and transferring personal information.

The Users of the digital resources of the school (including staff, students, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems are obliged to:

- Only use the login username and password that have been provided.
- Only accessing networks, data, or passwords that they are permitted to view, use, or copy.
- Holding off on disclosing personal information about oneself or others.
- Adhering to the network security procedures that are publicized and all school Internet filters (MDM).
- Notifying a network administrator or teacher of any security breaches or threats.
- Not harming networks, data, or other resources that do not legally belong to them without the owner's express consent.
- Sharing, safeguarding, and conserving these resources for other users.
- Reporting any issues with computers or networks to an administrator or staff member.
- Respecting copyright laws by not copying video, audio, or game content.
- Avoid plagiarism by giving credit to the authors of any work you use.
- Keeping your communication polite and courteous only.
- Notifying an administrator or teacher about any materials that seem dangerous or disturbing.
- Not intentionally accessing, transmitting, copying, or producing content (such as communications or content that are meant to harass, rude, threatening, pornographic, or discriminatory) that contravenes the school's code of conduct.
- Avoiding purposefully accessing, distributing, copying, or producing illegal content (e.g., stolen materials, obscenity, or illegal copies of works protected by copyright).
- Not misusing the resources to support illegal activity or behavior that goes against the school's code of conduct.
- Stay clear of chain letters, spam, and other uninvited bulk mailings.
- Not engaging in any commercial activity other than those authorized as school projects, such as purchasing, selling, or advertising.
- Create and publish webpages as well as other content using educational resources.
- Use electronic communication technologies like videoconferencing, chat, email, and text messaging.
- Install or download software, if also in conformity with laws and licenses.

Implications of Violation

Discipline up to and including the removal of the user's ability to access the school's IT resources may be imposed out for breaking these regulations. Depending on the seriousness and extent of the violation, further penalties, such as suspension or expulsion, may be applied in compliance with the school's code of conduct.

Reviewed by: SLT, CIDO, IT Engineer

Signed by the Principal:

Date:30/10/2023

Next Review Date: 01/09/2024

