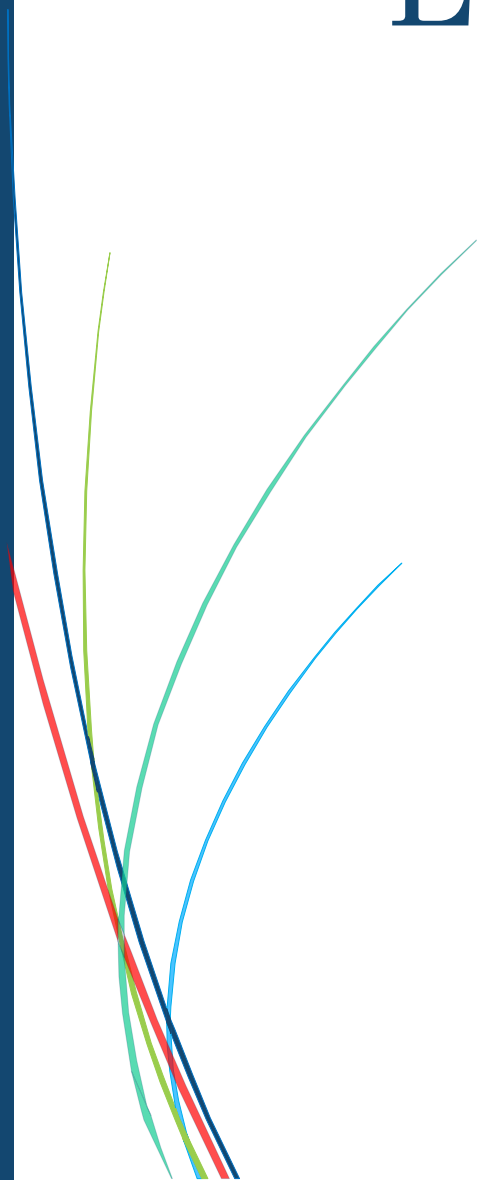
DEWVALE SCHOOL

E - SAFETY POLICY



E – SAFETY POLICY

Policy Name	E – Safety Policy	Policy No.	DWS_PLC_010
Effective Date	April 2024	Date of Last Review	NA
Date of Next Review	April 2025	Person in-charge	

INTRODUCTION

At Dewvale school Al Quoz, we recognize that excellence in education requires that technology is seamlessly integrated throughout the educational program and increasing access to technology is essential for that future. We also recognize that technology plays an important and positive role in everyone's lives, both educationally and socially. Through this policy we ensure that students, parents, and staff are aware of the risks attached to use and overuse of the internet, and are able to make educated choices regarding the risks.

AIMS

1. To implement and maintain a whole school approach to address the problem of cyber safety.
2. To make students aware of the safety issues regarding the internet, gaming, social networking, and online privacy.
3. To inform students about the negative consequences and provide them with skills and strategies for effective use of technology and protection of their digital identity.
4. To empower students to take ownership of and responsibility for their usage and habits.
5. To educate teachers about their role in ensuring that students are using the internet responsibly and safely.
6. To support parents in their efforts to ensure that their sons are using the internet responsibly and safely.

Definition: Cyber safety, refers to time allocated to use of the internet (and incorporates issues of gaming addiction). This includes the issues of safety around the internet - cyber bullying, identity theft etc. Few other safety issues include:

- Access to illegal, harmful or inappropriate messages.
- Unauthorized access to / loss of / sharing of personal information.
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing/distribution of personal images without an individual's consent or knowledge.
- Inappropriate communication/contact with others, including strangers.
- Cyber-bullying.
- Access to unsuitable video / internet games.
- An inability to evaluate the quality, accuracy and relevance of information on the internet.
- Plagiarism and copyright infringement.
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Education of pupil on E-safety

- Key E-safety Messages should be reinforced as part of a planned programme of assemblies/pastoral activities.
- Pupils 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.
- Pupils 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.
- Pupils 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 will be posted in the ICT suite.
- Staff should act as good role models in their use of ICT, the Internet and mobile devices.
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff

Responsibilities of school technical team

- All users have clearly defined access rights to the school ICT systems, they are provided with username and password, and are educated on their responsibility for the security of their passwords.
- Appropriate security measures are present to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices from accidental or malicious attempts which might threaten the security of the school systems and data.

Curriculum

- While using technology as a means of learning enrichment, students are guided to sites checked as suitable for their use.
- Students are monitored by the staff when they are required to conduct independent research in class. Students are taught to be critically aware of the material they access online, they are guided to validate the accuracy of information.

Responsibilities of the staff

- Staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images.
- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Written permission from parents or careers will be obtained before photographs of pupils are published on the school website.
- The official school email service is regarded as safe and secure and is monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems.
- Users must immediately report the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and pupils or parents / careers (email, chat, etc.) must be professional in tone and content.

Responsibilities of Students

- Students must not take, use, share, publish or distribute images of others without their permission.
- Always keep your profile private.
- Never accept friends you do not know in real life.
- Never post anything which could reveal your identity including photographs wearing a school uniform where possible.
- Never post anything you wouldn’t want your parents or teachers to see.
- Never agree to meet somebody you only know online without telling a trusted adult.
- Always tell someone if you feel threatened or someone upsets you. You may speak to your class teacher or the e-Safety Officer.
- Immediately report the receipt of any email that makes you feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.

Responsibilities of Parents

- Discover the Internet together.
- Agree with your child rules for Internet use in your home.
- Encourage your child to be careful when disclosing personal information.
- Talk about the risks associated with meeting online "friends" in person.
- Teach your child about evaluating information and being critically aware of information found online.
- Don't be too critical towards your child's exploration of the Internet.
- Let your children show you what they like to do online.
- Remember that the positive aspects of the Internet outweigh the negatives.

Bring Your Own Device (BYOD) Policy:

Dewvale school Al Quoz uses instructional technology as one way of enhancing our mission to teach the skills, knowledge and behaviours students will need as responsible citizens in the global community. Students learn collaboration, communication, creativity and critical thinking in a variety of ways throughout the school day. In an effort to increase access to those 21st Century skills, we will allow personal devices on our student network and school grounds for students.

Our school strives to provide appropriate and adequate technology to support instructional purposes. The use of personal devices by students is mandatory for Grades 2-5 and optional for Pre KG - Grade 1.

Device Types:

For the purpose of this program, the word "devices" will include: laptops, netbooks, IPads, and tablets. Please note that Nintendo DS, Smart phones and Tablet with SIM (and/or other gaming devices with internet access) is not permissible.

Guidelines:

- Students and parents/guardians participating in BYOD must adhere to the Student Code of Conduct from Remote Learning policy and e-Safety policy
- Each teacher has the discretion to allow and regulate the use of personal devices in the classroom and on specific projects.
- Approved devices must be in silent mode while on school campus, unless otherwise allowed by a teacher. Headphones may be used with permission from the teacher.
- Devices may not be used to cheat on assignments, quizzes, or tests or for non-instructional purposes.
- Students may not use devices to record, transmit, or post photographic images or video of a person or persons on campus during school hours or during school activities or in the school transport, unless otherwise allowed by a teacher.
- Devices may only be used to access computer files on internet sites which are relevant to the classroom curriculum.

Students and Parents/Guardians acknowledge that:

- The school's network filters will be applied to a device's connection to the internet and any attempt to bypass the network filters is prohibited.
- Dewvale school Al Quoz is authorized to collect and examine any device that is suspected of causing technology problems or was the source of an attack or virus infection.
- Students are prohibited from:
    - Bringing a device on premises that infects the network with a virus, Trojan, or program designed to damage, alter, destroy, or provide access to unauthorized data or information.
    - Processing or accessing information on school property related to "hacking." Altering or bypassing network security policies.
- Students and parents should be aware that devices are subject to search by school administrators if the device is suspected of a violation of the student code of conduct. If the device is locked or password protected the student will be required to unlock the device at the request of a school administrator.
- Printing from personal devices will not be possible at school.
- Personal devices must be charged prior to school and run on battery power while at school.

Lost, Stolen, or Damaged Devices:

Each user is responsible for his/her own device and should use it responsibly and appropriately. Dewvale school Al Quoz, takes no responsibility for stolen, lost, or damaged devices, including lost or corrupted data on those devices. While school employees will help students identify how to keep personal devices secure, students will have the final responsibility for securing their personal devices.

Usage Charges:

Dewvale school Al Quoz is not responsible for any possible device charges to your account that might be incurred during approved school-related use.

Network Considerations:

Users should strive to maintain appropriate bandwidth for school-related work and communications. All users will use the "WPSD STUD" wireless network to access the internet. WPSD does not guarantee connectivity or the quality of the connection with personal devices. Dewvale School Al Quoz Technology department is not responsible for maintaining or troubleshooting student tech devices.