مـــدرســـة ديـــرة الـدولـيـــة
DEIRA INTERNATIONAL SCHOOL

# E-safety Policy

2017-2018

The term 'MED' in this policy refers to any personal mobile electronic device (**excluding mobile phones**) with the capability to connect to the school's Wi-Fi network.

## Introduction

Deira International School is committed to supporting our community of students, parents/guardians and staff to understand both the benefits and risks of technology used in lessons, and to equip students with the knowledge and skills needed to be able to use technology safely and responsibly.

## What is e-safety?

E-safety is a term which means not only the internet but other ways in which students communicate using Mobile Electronic Devices (MED). E-safety is ensuring that students are protected from harm and supported to achieve the maximum benefit from new and developing technologies without risk to themselves or others.

The aim of promoting e-safety is to protect a young person from the adverse consequences of access or use of MED that includes bullying and inappropriate behaviour or exploitation.

It is the responsibility of students, parents/guardians and staff to understand the risks and acceptable use, as well as how to respond to incidents involving e-safety, both in and out of the school environment.

## Aims of the e-safety policy

- protecting and educating students and staff in their use of technology
- educating students, parents/guardians and staff about cyber-bullying, including the consequences
- informing teachers and parents/guardians about their role in safeguarding and protecting DIS students at school and at home
- putting 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

## Link to School Core Values and Aims

The e-safety policy is aligned to the following DIS Core Values and Aims:

### Core Values:

- guide and nurture individual development
- promote human rights and responsibility

### School Aim 1:

- maintaining an excellent learning environment with the best teaching resources available to us
- being open to new thinking and ideas
- using technology to enhance the learning experience

- recognising that different teaching methodologies are essential for effective learning to take place

School Aim 2:

- offering enjoyable and exciting approaches and opportunities to stimulate enthusiasm and motivation for learning
- promoting the importance of informed decision making

School Aim 3:

- promoting an ethos of mutual respect and support in the school community

## Teaching and Learning

The Internet is an essential tool in 21st century life for education, business and social interaction. DIS is committed to providing students with quality Internet access as part of their learning experience in order to raise educational standards and uphold the vision and mission of the school in creating exciting and innovative opportunities which promote student achievement and success.

Deira International School ensures that:

- students will be made aware of acceptable and unacceptable Internet use
- students will be taught, where appropriate, to be critically aware of the materials/content they access online and be guided to validate the accuracy of information
- students will be educated about the effective use of the Internet
- students will be taught how to evaluate Internet content by ICT teachers
- students will be taught how to report unpleasant Internet content to their class teacher, tutor or Head of Year
- the school Internet access is designed expressly for student use and includes filtering appropriate to the needs of our students
- where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites they visit
- the use of Internet-derived materials by students and staff complies with copyright law
- all students and staff understand the importance of password security and the need to log out of accounts

## Introducing the e-safety policy to students

- e-safety rules, in a format appropriate for our students, will be displayed in classrooms and discussed with students as part of their learning, where appropriate
- students will be reminded continuously and informed that school network and Internet use is monitored
- e-Safety and cyberbullying training will be embedded within the ICT teaching curriculum and Skills4Life programme

## Cyberbullying

DIS will engage proactively with students in preventing cyberbullying by:

- understanding and talking about cyber-bullying
- keeping policies and practices up to date with new technologies
- ensuring easy and comfortable procedures for reporting cyberbullying
- dealing with all bullying complaints and incidents following the procedures set out in the Anti-Bullying Policy
- promoting the positive use of technology
- warning students about not trusting unknown online users and teaching them what information is safe to share
- advising students to report immediately, to their tutors/Head of Year, the receipt of any communication that makes them feel uncomfortable, or is offensive, discriminatory, threatening or bullying in nature and not to respond to this form of communication in any way

## Cyber-bullying Related Sanctions

When staff/pastoral leaders are made aware of a cyberbullying incident that involves any of our students, the Primary/Secondary School Senior Leadership Team will:

- assess the immediate threat
- ensure the safety of the student (target) by separating the bully from the target and closely monitoring the situation
- demonstrate compassion and empathy to the student
- restrain the bully, if applicable
- investigate and gather evidence
- contact both student's parents
- notify key school staff
- enforce Anti-Bullying Policy 2014-2015 policy, as appropriate

The school will keep an evidence file of all cyber-bullying with screen shots, message logs or any other content, so that the seriousness of the behaviour and its negative impact on the school and learning environment can be demonstrated. This is vital, especially if the school intends to sanction students formally, e.g. suspensions, loss of extra-curricular privileges or inform parents.

Any students caught cyber-bullying, using obscene language, or taking photos to upload on social media sites in school will be placed immediately on a Red Behaviour Report (or its equivalent) with a possible outcome of suspension. They will also have their MED/mobile phone confiscated until the parent/guardian collects it.

## Social networking and personal publishing

The school has a duty of care to provide a safe learning environment for all its students and staff and will ensure the following:

- blocking student access to social media sites within school boundaries
- educating students about why they must not reveal their personal details or those of others, or arrange to meet anyone from an online site
- educating both students and staff as to why they should not engage in online discussion revealing personal matters relating to any members of the school community
- educating both students and staff about ensuring all technological equipment is always password/PIN protected
- informing staff not to accept invitations from students or parents/guardians on social media
- informing staff about regularly checking their security settings on personal social media profiles to minimise risk of access of personal information

## Students' images and work

Staff, parents/guardians and students need to be aware of the risks associated with publishing digital images on the internet. Digital images may remain on the internet forever and may cause harm or embarrassment to individuals.

- students' full names will not be used anywhere on the website, particularly in association with photographs
- photographs that include children will be selected carefully
- when using digital images, teachers should inform and educate students, where appropriate, about the risks associated with taking, sharing, publishing and distributing images
- at most school events, parents/guardians are welcome to take videos and digital images but these are for personal use only
- to respect everyone's privacy, school recorded images should not be published or made publicly available on any social networking sites
- any videos or digital images taken must insure that students are appropriately dressed and are not participating in activities that might bring the individual or the school into disrepute
- parents who do not wish to have their child photographed sign the school's 'no photograph statement' when first registering their child at DIS

## Dangers of Using Virtual Private Networks (VPN)

The usage of Virtual Private Networks (VPN) software is not allowed for the following reasons:

- The VPN is quite a discreet online tool, and the school can easily track and disable it, if a student is attempting to use it whilst connected to school Wi-Fi. However, this is not possible if you provide your child with 3G or 4G Network internet connection that allows downloading and using VPN services. This is where you, as parents, need to be more vigilant and check your child does not have a VPN app to access blocked sites.
- Students are not allowed to download and use software, utilities or other means to access internet sites or content that is blocked by the UAE's and school's internet/network filters. Usage of Virtual Private Networks (VPN) software is not allowed.
- The use of VPN in the UAE is illegal and can be punishable under the UAE law. While the UAE's Telecommunications Regulatory Authority has always maintained that the use of VPN is against its policies, now the police have once again cautioned that legal action can be taken under Law Number 9 against users of VPN.

## Enlisting parents' support

Parents will be made aware of the School's e-Safety Policy through an e-safety information evening, school newsletters and the Virtual Learning Environment (VLE) school page and via the school Website.

# Parent and Student e-Safety Consent Form

All students will have access to the school's computer facilities, including the internet, as an essential part of learning. Both students and their parents/guardians are asked to sign the following to show that the e-safety rules have been understood and agreed.

- As the parent or legal guardian of the student named below, I have read and understood the attached school rules and now grant permission for my son/daughter to use the internet, VLE and other ICT facilities at school.
- I know that my son/daughter has signed an e-safety agreement and they have a copy of the school e-safety rules on their VLE school page.
- We have discussed this document and they agree to follow the rules to support the safe and responsible use of ICT at school.
- I accept that the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies, but I understand that they will take every reasonable precaution to keep students safe and prevent students accessing inappropriate materials.
- I know the school has an educationally filtered service, restricted access email and provides age appropriate teaching around internet use and e-safety issues.
- I will support the school by promoting safe use of the internet and digital technology at home and will inform the school if I have any concerns over my child's e-safety.
- I understand that the usage of **Virtual Private Networks (VPN) software is not allowed**.

**Parent Name: _____**

**Parent Signature: _____**

**Student Name: _____**

**Student Signature: _____**

**Year: _____**

**Date: ____ / _____ / _____**

## Information system security

- school ICT systems, capacity and security are reviewed regularly by the IT team
- virus protection will be updated regularly

## Published content and the school website

- the contact details on the website are the school address, e-mail and telephone number. Staff or students' personal information will not be published
- the Whole School Educational Technology Coordinator and IT Manager will take overall editorial responsibility and ensure that content is accurate and appropriate

## Managing filtering

- if staff or students discover an unsuitable site, it must be reported to the Whole School Educational Technology Coordinator and IT Manager
- the IT Manager will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable

## Assessing risks

- the school will take all reasonable precautions to ensure that users access appropriate material only
- the school will revise continuously its e-safety policy to ensure that it is appropriate and that its implementation is effective

## Handling e-safety complaints

- complaints of Internet misuse will be dealt with by the Head of Year, Whole School Educational Technology Coordinator or Pastoral Deputy Principal
- complaints of a child protection nature must be dealt in accordance with school Child Protection Policy procedures and only by the designated Child Protection officers

## Staff and the e-safety policy

- all staff will be made fully aware of the importance of the DIS e-safety policy
- a copy of the policy will be available for all staff, parents/guardians and students
- staff will be made aware that Internet traffic can be monitored and traced to the individual user (discretion and professional conduct is essential)

## Staff ICT Acceptable Use Policy/ICT Code of Conduct

ICT and the related technologies such as email, the internet and MED devices are an expected part of our working life in school. This policy is designed to ensure all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to adhere to the content and sign below.

- I appreciate that ICT includes a wide range of systems and devices including mobile phones, PDAs, digital cameras, email, social networking and may include personal ICT devices when used for school business
- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- I understand that I am responsible for all activities carried out under my user name
- I will only use the school email, internet, VLE or any related technologies for professional purposes
- I will ensure that personal data is kept secure and used appropriately, whether in school, taken out of school or used remotely when authorised by the Principal
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory
- I will respect copyright and intellectual property rights
- Images of students and/or staff will only be taken, stored and used for professional purposes in line with school policy. Images will not be distributed outside the school network/VLE without permission
- I will ensure that my online activity both in school and outside school will not bring my professional role into disrepute
- I will ensure that all electronic communications with parents, students and staff are compatible with my professional role and that messages cannot be misunderstood or misinterpreted
- I will support the school's e-safety policy and help students to be safe
- I will report any incidents of concern regarding children's safety to the Child Protection Officer, the Whole School Educational Technology Coordinator or the IT manager
- I understand that sanctions for disregarding any of the above will be in line with the school's disciplinary procedures and serious infringements may be referred to the Police

I agree to follow the code of conduct and support the safe use of ICT throughout the school.

Full Name: _____

Job Title: _____

Signature: _____ Date: _____

## References

- www.swgfl.org.uk
- www.saferinternet.org.uk
- www.gov.uk
- www.thegrid.org.uk
- www.policy.e-safety.org.uk
- www.yeomanpark.notts.sch.uk

BED, June 2017

To be reviewed June 2018