Cyber-safety Policy

This policy is based on the school's values of Respect, Quality, Commitment and Diversity

Developed by: OHS&W Committee 2011	Reviewed annually: 2016	Next review: 2017

The overall goal of this policy is to create and maintain a cyber-safety culture that is in keeping with our values and with legislative and professional obligations. To this end, the following procedures are in place:

Access and Security

- Cyber-safety User Agreements must be in place for all children and students.
- Students must use the Internet in a safe and considerate manner.
- Students must follow the copyright and licensing laws with respect to software, information and other material retrieved from or published on the Internet.
- The School of Languages must make sure that children, students and staff are aware of the importance of ICT security and safety, and how to react properly and deal with ICT security incidents and weaknesses.
- The School of Languages must report to SAPOL if cyber behaviour is suspected to be an e-crime. A Critical Incident Form must also be submitted to DECD through IRMS.
- Staff will make a mandatory notification to the Child Abuse Report Line (13 1478) if they suspect child abuse and neglect.

The Department for Education and Child Development (DECD), through Technology & Knowledge Management Services, may record and monitor Internet use for the purposes of managing system performance, monitoring compliance with policies, or as part of disciplinary or other investigations. This applies to all users of the Department's online services, including children, principals and directors, educators, ancillary staff, volunteers and supervisors of students in any Departmental location, including schools.

User Identification and Passwords

- Given the unique nature of the School of Languages, students are authorised to use shared group user-IDs.
- Passwords must be kept confidential.
- Passwords must not be included in log-in scripts or other automated log-on processes.
- Passwords must not be disclosed to unauthorised people.
- Students will be accountable for any inappropriate actions (eg bullying, accessing or sending inappropriate material) undertaken by an unauthorised person using their password.

Appropriate Behaviour and Use

Students may use the Internet only for learning related activities that are approved by a teacher. They must not cause interference or disruption to other people or equipment, and students may not access or distribute inappropriate material. This includes:

- Distributing spam messages or chain letters
- Accessing or distributing malicious, offensive or harassing material, including jokes and images
- Bullying, harassing, defaming or giving offence to other people
- Spreading any form of malicious software (eg viruses, worms)
- Accessing files, information systems, communications, devices or resources without permission
- Using for personal financial gain
- Using non-approved file sharing technologies (eg Torrent)
- Using for non-educational related streaming audio or video
- Using for religious or political lobbying
- Downloading or sharing non-educational material.

This policy will be available on the school's web site. A report will be provided each term to the School Council about any school bullying data and trends, and any anti-bullying programs/initiatives in place or being considered. Relevant data will also be made available to the general school community via the school newsletter.

Cyber-safety Use Agreements

- Cyber-safety Use Agreements must be in place for all students. The age appropriate agreement must be agreed to and signed by the student and his/her parents.
- These agreements will be reviewed and updated yearly to ensure their appropriateness and effectiveness.

Glossary of Terms

Cyber-safety refers to the safe use of the Internet and ICT equipment/devices, including mobile phones.

Cyber bullying is bullying which uses e-technology as a means of victimising others. It is the use of an Internet service or mobile technologies - such as e-mail, chat room discussion groups, instant messaging, webpages or SMS (text messaging) - with the intention of harming another person. Examples include communications that seek to intimidate, control, manipulate, put down or humiliate the recipient.

Digital footprints are traces left behind by someone's activity in a digital environment. These traces can be analysed by a network manager or the police.

Sexting is where a person takes a sexually-explicit digital photograph of him or herself or of someone else, and sends it as an MMS or SMS via a mobile phone. These images can then be posted on the internet or forwarded electronically to other people. Once posted on the internet these images can leave a permanent digital footprint and be accessed at any time in the future. It is illegal to take sexual photos or videos of children and young people.

Social networking sites offer people new and varied ways to communicate via the Internet, whether through their computer or mobile phone. These sites allow people to easily and simply create their own online page or profile and to construct and display an online network of contacts, often called 'friends'. Users are able to build a network of connections that they can display as a list of friends. These friends may be offline actual friends or acquaintances, or people they know or have 'met' only online, and with whom they have no other link. Social networking sites are not limited to messaging, communicating and displaying networks. Nearly all sites allow users to post photos, video and often music on their profiles and share them with others.

ICT equipment/devices, as used in this document, includes but is not limited to computers (such as desktops, laptops, netbooks, PDAs), storage devices (such as USB and flash memory devices, CDs, DVDs, floppy disks, iPods, MP3 players), cameras (such as video and digital cameras and webcams), all types of mobile phones, gaming consoles, video and audio players/receivers (such as portable CD and DVD players), and any other similar technologies.

Inappropriate material in this document means material that deals with matters such as sex, cruelty, racism or violence in a manner that is likely to be injurious to children or incompatible with a school or preschool environment.

E-crime occurs when computers or other electronic communication equipment/devices (eg Internet, mobile phones) are used to commit an offence, are targeted in an offence, or act as storage devices in an offence. For further information for parents please refer to: http://www.esafety.gov.au/esafety-information/esafety-issues