ICT Appropriate Use Policy

Madeley Primary School
For the future

Table of Contents

ICT Appropriate Use Policy

RATIONALE

The *Melbourne Declaration on the Educational Goals for Young Australians* (MCEETYA 2008) recognises that in a digital age, and with rapid and continuing changes in the ways that people share, use, develop and communicate with ICT, young people need to be highly skilled in its use. To participate in a knowledge-based economy and to be empowered within a technologically sophisticated society now and into the future, students need the knowledge, skills and confidence to make ICT work for them at school, at home, at work and in their communities.

In the Australian Curriculum, students develop ICT capability as they learn to use ICT effectively and appropriately to access, create and communicate information and ideas, solve problems and work collaboratively in all learning areas at school, and in their lives beyond school. The capability involves students in learning to make the most of the digital technologies available to them, adapting to new ways of doing things as technologies evolve and limiting the risks to themselves and others in a digital environment.

At Madeley Primary we endeavour to provide opportunities and teach skills and understandings to ensure students gain educational benefit from ICT while reducing the risks relating to global access.

DEFINITIONS

- "Information and Communication Technology" (ICT) refers to technologies that allow access to information and ways to communicate information. It includes hardware (e.g. computers, mobile devices, smartwatches), software (e.g. programs, apps, webtools) and systems (e.g. Internet, email, phone).
- "ICT Services" refers to the school's network, wireless access and Internet.
- "Devices" refers to smaller ICT hardware including iPads, mobile phones, smartwatches, digital cameras.
- "Internet" refers to system that allows data to transfer around the world including the World Wide Web (anything accessed via a browser), email and instant messaging.
- "Cybersmart" is the term used to describe decisions online users make to be cyber safe.
- Cybersafety" refers to practices that ensure a safe online presence including limited sharing of personal details and personal images of yourself and others.
- "Netiquette" is the term used to describe Internet etiquette or online manners including using polite, non-offensive language, and photos.
- "1:1" refers to one computer or device per student. At Madeley Primary it is a parent-funded program where parents purchase of lease a Macbook for their child's use in Years 4-6.
- "Social Media" refers to any sites that allow sharing and comments of a social nature including photo and video sharing.

ICT Appropriate Use Policy

PRINCIPLES

1. At Madeley Primary School ICT is provided for educational purposes only.
2. Students are taught, and expected to follow, safe and appropriate ICT behaviours including cybersafety. Students shall take personal responsibility when using the school's ICT services by protecting their personal information and data, maintaining the required level of security, respecting the privacy of others, respecting the legal boundaries of licensing and copyright, and using language appropriate to the school's expectations. Students using ICT must not break State or Federal laws (a summary of these laws are included in this Policy and form part of this Policy.)
3. The school has the right to check all written, graphic, audio and other materials created, produced, communicated, stored or accessed on school ICT by students.
4. Students shall be made aware that access to ICT and in particular the Internet can expose them to inappropriate material or potential harm.
5. Students shall take personal responsibility when using the school's ICT devices and 1:1 devices by protecting and ensuring all equipment is treated with respect.

PROCEDURES

1. Madeley Primary School is committed to ensuring all students are aware of standards for the use of ICT within the school environment. Students and parents read and sign "Acceptable Use Agreements" that clearly outline expected behaviour when using ICT at school. Consequently, unacceptable use will not be tolerated under any circumstances and further education and disciplinary action will be taken against any student who breaches these agreements.
2. Madeley Primary explicitly teaches cybersmart behaviours as part of the Health program and on a needs basis. Cybersmart is the government online safety resource http://www.cybersmart.gov.au/ .
3. Madeley Primary provides parent information through class notes, school newsletters and class websites.
4. Madeley Primary School is committed to regularly updating this policy.

Acceptable use includes but is not limited to:

- Applying social and ethical protocols and practices when using ICT e.g. cybersafety, netiquette
- Investigating with ICT e.g. conducting research, analysing data
- Creating with ICT e.g. creating multimedia products
- Communicating with ICT e.g. email, online discussion, social media
- Managing and operating ICT e.g. file management, operating ICT devices

For more information http://www.australiancurriculum.edu.au/generalcapabilities/information-and-communication-technology-capability/introduction/introduction

Unacceptable use includes but is not limited to:

- Accessing networks without school authorisation;
- Transmitting or deliberately accessing and/or receiving material that may be considered inappropriate, which includes threatening, sexually explicit, or harassing materials, offensive or discriminatory materials, or material that may be harmful either physically or emotionally, which includes bullying or harassment of fellow students or others outside the school;
- Communicating information concerning any password, identifying code or other confidential information or violating the security of the system in any way;
- Using personal devices (i.e. mobile phones, smartwatches) during school times
- Interfering with or disrupt network users, services or equipment. Disruptions include but are not limited to, distribution of unsolicited advertising, propagation of viruses, in any form, "Jail Breaking" mobile devices and using the network to make unauthorised entry to any other machine accessible via your network;
- Plagiarising and/or breaching copyright laws, including software copyright and re-engineering of software;
- Conducting private business matters or use the system for any personal gain; and,
- Downloading and/or installing software programs (eg. dmg files), apps, videos, music, picture galleries, copying music CD's, screen savers and games, etc. without the permission of the school.
- Inviting or accepting a School staff member to be a 'friend' on social networking sites (such as Facebook or Instagram). *Note: an online communication or e-learning site that a staff member manages that is not managed by DOE (eg. wiki, blog, Spelling City, Study Ladder) is acceptable as long as its primary purpose remains education-related.*
- Defame someone or an organisation;
- Undertake activities that breach State and Commonwealth laws.

MOBILE ELECTRONIC DEVICES

Mobile electronic devices include such devices as mobile phones, smartwatches, iPads, personal computers, video and digital cameras and graphics calculators.

- Students who bring devices to school will hand them into the care of the class teacher at the start of the day, unless it is being used for educational purposes, to be stored securely.
- Smartwatches may be worn, they must be turned onto aeroplane mode.
- No calls or messages are to be made or taken during school time. Calls by and to parents are to be directed through Administration.
- Only approved 1:1 Macbooks will be registered to use the school network.
- The School will not be responsible for the loss, misuse or damage of privately owned electronic devices, or any other valuables.
- Any School-owned mobile device must be treated with the utmost care and respect at all times. Any damage must be reported to the Classroom teacher or ICT Technician immediately.
- Any damage to personal devices must be reported to the Classroom teacher or parents immediately.

EMAIL MONITORING

All students and parents should be aware that Madeley Primary School and the Department of Education WA may monitor student email. All students in Department of Education Schools in Western Australia are subjected to this filtering. School administration and teachers can deny access to students found to be using the DOE email service inappropriately.

INTERNET USE

All data use is closely monitored. Any students abusing the available bandwidth will have their internet access revoked, ensuring that access for everyone is responsive and fair. The Education Department of Western Australia filters the internet for inappropriate sites and blocks them from student access. However the system is imperfect and as such students and parents should be aware that all internet traffic is monitored and logged. Safe Internet use also requires students to make responsible decisions learned through cybersafety lessons.

STUDENT PASSWORDS

All students are issued with a username and password at the commencement of enrolment. These passwords are for individual student use ONLY and as such they should not be given to any other student at the School. Students are responsible for protecting their individual password. Passwords can be changed by the individual or admin/teachers.

Your username and password gives you access to:

- The Madeley Primary School network
- School owned computers (IT Labs and Learning area trolleys)
- Connect
- Your email @student.education.wa.edu.au

Disclosing passwords leads to other students having access to student email and any activity performed on the network will be logged against the incorrect student.

Students who use another student's password will be deemed to be in breach of this policy. If a student suspects their password security has been breached the student should immediately change their password when possible and report this occurrence to the ICT Technician or Classroom teacher. A new password may be issued and further misuse of the password may be monitored and dealt with as necessary.

LEGAL IMPLICATIONS

Users are advised that the inappropriate use of electronic information can be a violation of State and Federal laws. Please make yourself aware of the statutes that are applicable to your use of the School ICT facilities.

IMPORTANT STATUTES THAT ARE APPLICABLE TO STUDENTS

Copyright Act 1968 (Cth)

Students may copy or otherwise deal with copyright material for the purpose of study or education. However, generally only the author of original material has the right to reproduce, copy, publish, perform, communicate to the public and make an adaptation of the copyright material.

Equal Opportunity Act 1984 (WA)

This Act precludes:

1. Discrimination against persons on grounds of sex, marital status or pregnancy, family responsibility or family status, sexual orientation, race, religious or political conviction, impairment or age in education.
2. Sexual harassment and racial harassment in the workplace and in educational institutions, and
3. Promotes community recognition and acceptance of the equality of all persons regardless of their face, sexual orientation, religious or political convictions, impairments or ages.

Censorship Act 1996 (WA)

Students must not use a computer service to transmit, obtain or request an article knowing that it contains objectionable and restricted material. It is an offence to possess or copy indecent or obscene articles or child pornography. Students should be aware for their own protection that people who deal with such material commit an offence.

Criminal Code 1913 (WA)

Students should be aware that it is illegal to show offensive material to children under 16, and that if someone does show them offensive material that person is committing an offence. Racist harassment and incitement to racial hatred are also criminal offences.

Cybercrime Act 2001 (Cth)

Unauthorised access to or modification of data held in a computer and unauthorised impairment of electronic communication, eg. ‘hacking’ or infecting computer systems with a virus, are illegal.

Privacy Act 1988 (Cth)

Students should respect that the personal information of others is private. This Act covers the collection, use and disclosure, quality and security of personal information.

Evaluation:

This policy will be reviewed as part of the school’s review cycle.

Last update: November 2023