ICT Acceptable Use Policy

Rationale for use of ICT

Milgate Primary School (MPS) is providing students access to the school's electronic network. This network includes Education Department Internet access, email, computer services, videoconferencing, computer equipment, mobile devices, iPads and related equipment / software for educational purposes. The purpose of this network is to prepare students for success in life and work in the 21st century. This policy is to protect the safety and wellbeing of all users.

What is covered

This policy covers both equipment and networks used at the school.

Equipment includes school issued and personal devices taken and used at school such as mobile phones, computer, ipads and notebooks, interactive data panels, projectors, digital cameras, ipods, printers, scanners, microphones and headphones.

Network covers internet (world-wide web) and school (intranet) networks and mobile phone networks.

For outside school equipment and networks, parents should consider implementing a similar policy for student safety and well-being. Please see Annex B for additional guidelines and advice.

The Policy:

When using ICT equipment and networks, students are expected to be:

1. Responsible – students will not do anything that violates the law
2. Respectful – students will look after equipment and care about other users
3. Effective – students should use the equipment to support learning

Principle	Examples of what this looks like
Responsible	Students should not send or view illicit, fraudulent, obscene or pornographic material. Students must not violate copyright law and correctly reference copyright material.
Respectful	Students should not engage in defamation, harassment and abusive behaviour. Students should not embarrass themselves or other users when using social media, chat rooms or other online activity.

Effective	Students should use ICT to support learning; leisure activities (playing games, participating in social media) is allowed as long as it does not interfere with research and learning activities.

This policy is consistent with the school's eSmart policy, a comprehensive Cyber Safety Program designed by the Education Department and the The Alannah and Madeline Foundation. The program is a whole-of-community approach to monitoring, modelling and correcting behaviour.

Monitoring - antivirus, internet filters, and log files will be used to monitor usage and teachers have the right to oversee any file on a student's equipment.
Modelling – teachers will model correct and safe (including OH&S) use of ICT for learning
Correcting – students will be supported for correct behavior.

Breaches to the ICT Acceptable Use Policy

All issues will be investigated by the teacher and reported to the principal. In all cases, students will be offered protection and support. Depending on the level of threat, parents may be notified and DEECD policy followed for resolution. Failure to adhere to the ICT Acceptable Use Guidelines can result in:

- the student forfeiting their privilege to be part of the Milgate Primary School Electronic Network
- deleting of apps
- removing the equipment from the student

Evaluation

This policy will be reviewed as part of the school's three year review cycle.

Annex A: Acceptable Use Agreement

Student Agreement

Name: _____ Class: _____

I have read with my parents the Milgate Primary School Acceptable Use ICT Policy. I agree to use the equipment and networks responsibly, respectfully and effectively.

I understand that failure to follow this Acceptable Use ICT Policy may result in me having my privilege suspended or revoked.

Student Signature: _____ Date: _____

Parent Agreement

I have read the Milgate Primary School Acceptable Use ICT Policy. I give permission for my child to participate.

I understand that failure to follow this Acceptable Use ICT Policy may result in my child having his / her privilege suspended or revoked.

Parent Name: _____

Parent Signature: _____ Date: _____

Annex B: Recommendations & Guidelines for parents

At school computers and the Internet is mostly used to support teaching and learning. At home, however, it is often used differently. Not only is it a study resource for students, but it is increasingly being used as a social space to meet, play and chat. The Internet has some really tricky ways to lead people into websites they never meant to visit. It is easy for us all to get distracted. Unfocused clicking through websites can lead to inappropriate content. Below are some guidelines for parents to embrace these technologies, while being aware of the pitfalls.

Open communication between parents, teachers and students is the best way to keep students safe. It is important that students feel that it is ok to tell a teacher or parent when they are feeling uncomfortable or threatened online. Parents should play an active role in monitoring and restricting their use.

Monitor

Make some time to sit with your child to find out how they are using the Internet and who else is involved in any online activities. Ask questions when your child shows you what they are doing, such as:

- who is else is sharing this space or game - did you know them before or "meet" them online?
- why is this so enjoyable – what makes it fun?
- can you see any risks or dangers in the activity - what would you say to warn/inform a younger child?
- what are you doing to protect yourself or your friends from these potential dangers?

Have the computer with Internet access in a shared place in the house and encourage your child to approach an adult for help. Limit the time your child spends on electronic devices each day. Collect all handheld devices at an allocated time each evening (eg. 7pm) and store them in a central location.

Privacy

Students can be approached, groomed, and bullied online. They also love to publish information about themselves and their friends in spaces like Myspace, blogs etc. We recommend they:

- don't use their own name, but develop an online name and use avatars.
- don't share personal details including images of themselves or their friends online
- password protect any spaces or accounts they have and protect that password.
- don't allow anyone they don't know to join their chat or collaborative space.
- are reminded that any image or comment they put on the Internet is now public (anyone can see, change or use it)
- set all profiles and accounts to private.

Illegal behaviours

All music, information, images and games on the Internet are owned by someone. A term called copyright is a legal one and has laws to enforce it. By downloading a freebee you risk bringing a virus or spyware to the computer or system. These can destroy a computer system or provide hackers with details such as passwords and bank accounts.

Additional Resources

eSmart Schools

eSmart Schools was developed by RMIT University in consultation with cybersafety, bullying, education and industry experts from across Australia.

https://www.esmartschools.org.au

Cybersmart

Cybersmart is a national cybersafety and cybersecurity education program managed by the Australian Communications and Media Authority (ACMA), as part of theAustralian Government's commitment to cybersafety.

http://www.cybersmart.gov.au/kids.aspx

Bullying. No Way!

Bullying. No Way! is managed by the Safe and Supportive School Communities (SSSC) Working Group. The SSSC includes education representatives from the Commonwealth and all states and territories, as well as national Catholic and independent schooling representatives. Members work together to create learning environments where every student and school community member is safe, supported, respected and valued.

http://bullyingnoway.gov.au/parents/facts/cybersafety.html

Stay Smart Online

Stay Smart Online is the Australian Government's online safety and security website, designed to help everyone understand the risks and the simple steps we can take to protect our personal and financial information online.

https://www.staysmartonline.gov.au/home_users/protect_your_children