•Milkwood•
Steiner School

Digital Safety

POLICY

Policy Category: WHS and Wellbeing	**Document ID:**
Number of pages: 7	**Appendices:**
Version: 1.1	**Status:** Approved
Reviewed by: Principal	**Endorsed by:** Board via chair
Approved by: Board	**Date:** ~~30 JAN 2025~~ 11/5/25
Signature:	
Recommended frequency of review: 1 year for new policies, and then at least every 3 years unless otherwise approved by the Executive Team. Next review: 2028	
Location on shared drive:	
Related Legislation and Documents: *eSafety Commission's Best Practice Framework for Online Safety Implementation* *Privacy Policy* *Emergency Management Policy* *Communication Policy* *Critical Incident Policy* *WHS Policy* *Child Protection Policy* *Code of Conduct* *Discipline Policy*	
Published to:	
Additional Information:	

Document history:

Version	Date	Nature of Amendment
1.0	2024	New Policy created due to the use of digital devices in classrooms with the introduction of Middle School.
1.1	30/1/25	No changes

Digital Safety

DEFINITIONS AND ABBREVIATIONS

MSSA: Milkwood Steiner School Association

ICT: Information and Communications Technology.

PURPOSE

This policy exists to ensure online safety of students at Milkwood Steiner School and to establish clear mechanisms to prevent, identify and respond to incidents of concern involving students, online, at school. This policy acknowledges that

1. Digital safety is based on recognising, acknowledging and understanding rights and responsibilities in the digital age.
2. Digital safety positively frames the use of technology, while also building awareness of factors that decrease and increase the risk of harm.
3. Digital safety is underpinned by effective whole-school approaches for promoting student wellbeing and preventing student harm.
4. Digital safety builds knowledge and skills across the curriculum. It includes both technical and relational (interpersonal) aspects needed to navigate digital environments and develops student agency to use what they have learned in practice
5. Digital safety is continuously improved using the best available evidence, data and authoritative information from eSafety about online safety issues, risks and harm.

SCOPE

This document applies to all areas of the school, including the Milkwood Steiner School Association Board (the Board), staff, students, Playgroup, After School Care, families, carers and friends of MSSA, volunteers and visitors to the school.

This policy is particularly relevant to students from Class 6-8 who use digital technologies in class to meet curriculum expectations. It is also particularly relevant to students who use devices as assistive technology.

This policy applies to all school context, while in school or off site.

POLICY STATEMENT

ICTs can be creative and necessary tools.

At Milkwood, ICT is not used in the Early Childhood or Primary years, unless required as assistive technology and incorporated into an EAP. Prior to Middle School years, teaching should not incorporate recorded music, videos or other technology.

In exceptional, one-off circumstances, a limited, purposeful use of ICT may be considered in the Primary School years for teaching purposes when no alternative is available and students cannot access a particular learning experience without it, to their detriment. This requires the approval of the Principal.

Targeted, meaningful, purposeful projects using computers are introduced from Year 7 (Middle and High School).

Middle and High School students who own their own laptops may be permitted to bring these in for targeted use, at the recommendation of the teacher, with the approval of the Principal and in accordance with Milkwood's policies. Personal devices may only be used by the student who owns them, and must follow the same rules and conditions as any school device in use.

Reducing the impact of media and technology on our students includes an expectation that staff model *appropriate and minimal use of technology in the classroom.*

Staff carry mobile phones for emergency contact only. Staff must not use their phones for any other purpose when working with children. This includes taking photos/videos, social media, or accessing the internet.

Examining electronic devices

The Principal has the specific power under the Education and Inspections Act 2006 and Education Act 2011 to search for and if necessary, delete inappropriate images or files on students' electronic devices, including but not limited to mobile phones, tablets and laptops/computers where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, the Principal must reasonably suspect that the data or file in question has been, or could be used to:

1. Cause harm, and/or
2. Disrupt teaching and learning, and/or
3. Break any school rules.

If inappropriate material is found on a device, the Principal may

1. Delete that material, or
2. Retain the device as evidence (of a criminal offence or breach of school policy), and
3. Report to the police

Any complaints about searching or deleting inappropriate images or files on students' electronic devices may be received according to the Communications and Grievance Policy.

The Critical Incident Policy guides the school's response to digital safety breaches of serious concern.

Device Agreements

Students who use devices at school must sign an agreement regarding the acceptable use of the school's ICT systems and the internet, and the use of their own devices. The agreement must also be signed by their parent/guardian.

The Principal is responsible for updating this agreement according to changing advice from the eSafety Commissioner and the safety needs of the school. An example agreement is provided in the Digital Safety Policy Guidelines.

Acceptable use of devices and the internet at school

Use of the school's internet for all students, staff and volunteers must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

Students must submit all devices, including phones, to the front office on arrival at school. Unless approved by the Principal for educational purposes, students may not bring their own devices or phones into school. Students breaching this expectation may have their phones confiscated and available for a parent/carer to collect.

Milkwood Staff are allowed to bring personal phones and devices into school but their use should be limited to emergency contact. Staff must not take photos or recordings on personal devices at school.

School cameras are provided to each class for the purpose of documenting learning for educational purposes, and for promotional purposes for the school and the cameras and their data should only be used in accordance with the school's Privacy policy, Child Protection policy and all other policies.

The Principal is responsible for

- Creating digital safety and device agreements made with students, families and teachers
- Leading the response to online safety incidents according to the *Critical Incident Policy* and *Emergency Management Policy*
- Ensuring that any incidents of cyber-bullying or any other conduct and behaviour concerns online are dealt with in line with the school's Code of Conduct and Discipline Policy.
- Ensuring that relevant staff have access to training and information in online safety

Teachers are responsible for

- Maintaining their professional skills to allow them to safely incorporate digital technology in their classes
- Incorporating digital technologies into learning tasks in ways that are purposeful, targeted, supervised and safe
- Ensuring that students in their care adhere to this policy
- Implementing digital safety instruction for their class or for any individual student in their class who has been approved to use digital devices at school

The Finance Manager is responsible for

- Ensuring the schools digital assets, including but not limited to school computers, cameras and devices, are equipped with appropriate filtering and monitoring systems which are updated and reviewed regularly to keep students safe from harm and inappropriate content and contact online while at school
- Ensuring the school's ICT systems are secure and protected against viruses and malware, and that safety mechanisms are updated regularly
- Conducting regular security checks and monitoring the school's ICT systems
- Ensuring that access to potentially dangerous sites and downloads are blocked on the school's digital assets.

Parents are responsible for

- Supporting children Primary and Early Childhood to not engage with screen-based technology in their Primary years, at home. By sending your child to Milkwood Steiner School, parents commit to their child being "screen-free" at home on school days.
- If students are using their own, approved devices at school, ensuring that these devices meet the school's expectations for digital safety
- Signing their child's digital safety agreement, along with their child.

Staff, parents, volunteers, students, visitors and MSSA members are responsible for notifying the Principal of any concerns or questions regarding digital devices and safety.

Guidelines

Milkwood Steiner School's Student Device Agreement

Name of student:

I agree to:

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, and with a teacher's permission
- Keep my username and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name or any contact details to anyone without the permission of my teacher and parent/guardian
- Tell a teacher or another trustworthy adult immediately if I find any material which might upset, distress or harm me or others
- Always log off or shut down a computer when I'm finished using it
- Not access any inappropriate websites including: social networking sites, chat rooms, gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Not open any attachments in emails or follow any links in emails, without first checking with a teacher
- Not use any inappropriate language when communicating online, including in emails
- Not log in to the school's network using someone else's details
- Not arrange to meet anyone offline without first consulting my parent/guardian and teacher, or without adult supervision
- If bringing a personal phone or device to school, I will submit it to the front office on arrival or make sure I have the Principal's approval to bring it into class if my teacher agrees. I will use it responsibly and will not access any inappropriate websites or any other inappropriate material or use inappropriate language when communicating online
- I agree that the school will monitor anything I may access online and there will be consequences if I don't follow the rules.

Student's signature

Date

Parent/Guardian agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for students and for my child using the school's ICT systems and internet and for using personal electronic devices in school and will make sure my child understands these.

Parent/Guardian's signature

Date