



# Digital Technologies Acceptable Use Agreement

## Policy

Policy review team members: Lisa Grgic, Bev Harvey, Michelle Polley, Jodie Prendergast, John Bothe, Dean Charge, Jane Herring, Kate Eadie, Katanya Barlow and Nathan Goodrick.

This policy was last ratified by School Council on 1<sup>st</sup> June 2020 and due for review in 2021.

### Rationale:

At Mt Eliza Primary School we support the right of all members of the school community to access safe and inclusive learning environments, including digital and online spaces. This agreement outlines the School's roles and responsibilities in supporting safe digital learning, as well as the expected behaviours we have of our students when using digital or online spaces. The agreement also applies during school excursions, camps and extra-curricula activities.

### Aims:

To ensure that all students and members of our school community understand:

- (a) our commitment to providing students with the opportunity to benefit from digital technologies to support and enhance learning and development at school, including our 1-to-1 personal device program.
- (b) expected student behaviour when using digital technologies including the internet, social media, and digital devices (including computers, laptops, tablets)
- (c) the school's commitment to promoting safe, responsible and discerning use of digital technologies, and educating students on appropriate responses to any dangers or threats to wellbeing that they may encounter when using the internet and digital technologies
- (d) our school's policies and procedures for responding to inappropriate student behaviour on digital technologies and the internet.

### SCOPE

This policy applies to all students at Mt Eliza Primary School. Staff use of technology is governed by the Department's *Acceptable Use Policy*.

### DEFINITIONS

For the purpose of this policy, "digital technologies" are defined as being any networks, systems, software or hardware including electronic devices and applications which allow a user to access, receive, view, record, store, communicate, copy or send any information such as text, images, audio, or video.

Mt Eliza Primary School uses the internet and digital technologies as teaching and learning tools. We see the internet and digital technologies as valuable resources and acknowledge they must be used responsibly.

### Vision for digital technology at our school

Mt Eliza Primary School understands that safe and appropriate use of digital technologies including the internet, apps, computers and tablets provide students with rich opportunities to support learning and development in a range of ways.

Through increased access to digital technologies, students can benefit from enhanced learning that is interactive, collaborative, personalised and engaging. Digital technologies enable our students to interact with and create high quality content, resources and tools. It also enables personalised learning tailored to students' particular needs and interests and transforms assessment, reporting and feedback, driving new forms of collaboration and communication.



Mt Eliza Primary School believes that the use of digital technologies at school allows the development of valuable skills and knowledge and prepares students to thrive in our globalised and inter-connected world. Our school's vision is to empower students to use digital technologies safely and appropriately to reach their personal best and fully equip them to contribute positively to society as happy, healthy young adults.

## Implementation:

### Safe and appropriate use of digital technologies

Digital technology, if not used appropriately, may present risks to users' safety or wellbeing. At Mt Eliza Primary School, we are committed to educating all students to be safe, responsible and discerning in the use of digital technologies, equipping them with skills and knowledge to navigate the digital age.

At Mt Eliza Primary School, we:

- use online sites and digital tools that support students' learning, and focus our use of digital technologies on being learning-centred
- restrict the use of digital technologies in the classroom to specific uses with targeted educational or developmental aims
- supervise and support students using digital technologies in the classroom
- effectively and responsively address any issues or incidents that have the potential to impact on the wellbeing of our students
- support parents and carers to understand safe and responsible use of digital technologies and the strategies that can be implemented at home through the implementation of Digital Technology Information Evenings.
- have programs in place to educate our students to be promoting safe, responsible and discerning use of digital technologies, including the implementation of cyber safety digital programs, such as *Hector's World* <https://www.esafety.gov.au/educators/classroom-resources/hectors-world> and *Cybersmart Challenge* <https://www.esafety.gov.au/educators/classroom-resources/cybersmart-challenge>
- educate our students about digital issues such as online privacy, intellectual property and copyright, and the importance of maintaining their own privacy online
- actively educate and remind students of our *Student Engagement* policy that outlines our School's values and expected student behaviour, including online behaviours
- have an Acceptable Use Agreement outlining the expectations of students when using digital technology at school
- use clear protocols and procedures to protect students working in online spaces, which includes reviewing the safety and appropriateness of online tools and communities, removing offensive content at earliest opportunity
- educate our students on appropriate responses to any dangers or threats to wellbeing that they may encounter when using the internet and other digital technologies
- provide a filtered internet service to block access to inappropriate content
- refer suspected illegal online acts to the relevant law enforcement authority for investigation
- Distribution of school owned devices to students and personal student use of digital technologies at school will only be permitted where students and their parents/carers have completed a signed Acceptable Use Agreement.

It is the responsibility of all students to protect their own password and not divulge it to another person. If a student or staff member knows or suspects an account has been used by another person, the account holder must notify the classroom teacher or school leader as appropriate, immediately.

### Messaging

All messages created, sent or retrieved on the school's network are the property of the school. The school reserves the right to access and monitor all messages and files on the computer system, as necessary and

appropriate. Communications including text and images may be required to be disclosed to law enforcement and other third parties without the consent of the sender.

On any given school day, parents or carers are not permitted to send messages to students which can be retrieved on a student iPad or similar tablet device between the school hours of 8:45am – 3:15pm, to avoid any distractions from student learning.

If a parent needs to give a child a message, they must contact the staff in the office. If a parent sends a message to a child's iPad during school hours, the teacher will contact the parent and remind them of the details in the Digital Technologies Acceptable Use Agreement. If it happens a second time, the parent will be contacted by a member from the school leadership team. If it occurs a third time, the device will be removed from the student for a period of time.

### **Student behavioural expectations**

When using digital technologies, students are expected to behave in a way that is consistent with Mt Eliza Primary School's *Statement of Values, Student Wellbeing and Engagement policy*, and *Bullying Prevention policy*.

When a student acts in breach of the behaviour standards of our school community (including cyberbullying, using digital technologies to harass, threaten or intimidate, or viewing/posting/sharing of inappropriate or unlawful content), Mt Eliza Primary School will institute a staged response, consistent with our policies and the Department's *Student Engagement and Inclusion Guidelines*.

Breaches of this policy by students can result in a number of consequences which will depend on the severity of the breach and the context of the situation. This includes:

- removal of network access privileges
- removal of email privileges
- removal of internet access privileges
- removal of printing privileges
- other consequences as outlined in the school's *Student Wellbeing and Engagement and Bullying Prevention policies*.

### **iPads at Mt Eliza Primary School**

Classes from grade prep – grade 4 at Mt Eliza Primary School have access to iPad and laptop devices for educational purposes. Students in grade 5 and grade 6 also have access to laptop devices, but must bring a charged iPad to school each day to be used during class time for different learning activities.

Our school operates a Bring Your Own Device (BYOD) program, which means students must bring their own purchased or leased iPad with them to school each day.

Please note that our school does not have insurance to cover accidental damage to students' iPads, and parents/carers are encouraged to consider obtaining their own insurance for their child's iPad.

Mt Eliza Primary School has in place arrangements to support families who may be experiencing long or short-term hardship to access iPads for schoolwork. We also have a number of spare iPads that can be loaned to students in certain circumstances. These will only be accessible at school.

Students, parents and carers who would like more information or assistance regarding our BYOD program are encouraged to contact the classroom teacher.

### **Review Cycle**

This policy was last updated on 1<sup>st</sup> June 2020 and is scheduled for an annual review in June 2021.

## ANNEXURE A: ACCEPTABLE USE AGREEMENT

### 2020 MT ELIZA PRIMARY SCHOOL Acceptable Use Agreement for Internet and Digital Technologies

Mt Eliza Primary School believes the teaching of cyber safety and responsible online behaviour (digital citizenship) is essential in the lives of students and is best taught in partnership between home and school.

Students of the 21st century spend increasing amounts of time online, learning and collaborating. To be safe when online and to gain the greatest benefit from the opportunities provided through an online environment, students need to do the right thing by themselves and others online, particularly when no one is watching.

Safe and responsible behaviour is explicitly taught at our school and parents/carers are requested to reinforce this behaviour at home.

Some online activities are illegal and as such will be reported to police.

Mt Eliza Primary School uses the internet and digital technologies as teaching and learning tools. We see the internet and digital technologies as valuable resources, and acknowledge they must be used responsibly.

#### Part A - School support for the safe and responsible use of digital technologies

Your child has been asked to agree to use the, internet and mobile technologies responsibly at school. Parents/carers should be aware that the nature of the internet is such that full protection from inappropriate content can never be guaranteed.

At Mt Eliza Primary School we support our school community by:

- Year 5-6 students using Seesaw (online learning portal)
- grades using Class Dojo as a communication/behaviour management tool
- utilising digital citizenship resources from ACMA (Australian Communication and Media Authority) and DET to support teacher programs
- following guidelines from DET Bully Stopper Program
- P-6 students involved in cyber safety programs provided by the federal government- *Hector's World* <https://www.esafety.gov.au/educators/classroom-resources/hectors-world> and *Cybersmart Challenge* <https://www.esafety.gov.au/educators/classroom-resources/cybersmart-challenge>
- providing parent information sessions focused on cyber safety principles.

In addition to this our school:

- has policies in place that outline the values of the school and expected behaviours when students use digital technology and the internet
- provide a filtered internet service and secure school network
- provide access to the Department of Education and Training search engine Connect ([www.education.vic.gov.au/primary](http://www.education.vic.gov.au/primary) or [www.education.vic.gov.au/secondary](http://www.education.vic.gov.au/secondary)) which can be used to direct students to websites that have been teacher recommended and reviewed
- provide supervision and direction in online activities and when using digital technologies for learning
- support students in developing digital citizenship skills
- provide cyber safety programs which are reinforced across the school
- use mobile technologies for educational purposes (e.g. podcasts or photos from excursions) across the school (Grade 5 and 6 1:1 iPad program and iPads in P-2 area)
- provide support to parents/carers to understand this agreement (e.g. language support)
- provide support to parents/carers through information evenings and through the document attached to this agreement for parents to keep at home.

When aspects of the Student Acceptable Use Agreement have been breached, the following management plan will be implemented (in accordance with our behavioural management plans):

**Misdemeanours for inappropriate use of iPads and similar devices can include:**

- The use of iPads and similar devices being used when not under the direct supervision of the teacher on the school grounds
- Using a virtual private network (VPN) application or similar technologies designed to circumvent the school's secure network
- The use of 3G or 4G mobile WIFI on a device is not allowed. Only the school network is to be used by students while at school
- Using the iPad camera when not under the direct supervision of the teacher
- Electronic devices not remaining in their protective covers
- Electronic devices are left in an unsafe space, vulnerable to damage (on the floor, on the edge of the table)
- Non approved games or entertainment are not permitted during school time
- Music is not able to be listened to during classes or study, unless used for learning as directed by teacher
- Students should not touch or use the device of another person without their permission
- Inappropriate use of the school network, or attempting to access the school network via another person's login and username
- Giving personal details to others, such as passwords, lock codes, or locker padlock codes is strictly prohibited
- Do not use iMessage, Instagram, Skype, Kik or any chatrooms or social media while at school
- Do not send or use of inappropriate or explicit language, photos or images
- Posting of photos or videos of other students in school uniform or other identifying features, or staff on social media is not allowed
- Transmission or sharing of copyrighted or pirated apps is strictly prohibited
- Accessing or sharing of offensive, profane, threatening, pornographic, obscene or sexually explicit materials is strictly prohibited
- Spamming other users is not allowed
- Using the school's internet or email accounts for financial or commercial gain, or for any illegal activity is not allowed
- Engaging or participating in credit card fraud, electronic forgery, ID theft, or other forms of illegal behaviour
- Vandalising other student iPads or school equipment
- Attempting to bypass the school filtering system via any means
- Taking the iPad out of school bag before school, during recess and lunch and after school on the school grounds without teacher supervision.

**Consequences for misdemeanours and inappropriate use of mobile devices**

- All students at Mt Eliza Primary School have a right to use the extensive Mobile Technologies available to them. They also have a responsibility to use it sensibly and maturely. Should students not do this, the following system of consequences will be applied as appropriate.
- ***First Offence - Verbal warning to student, name recorded by classroom teacher.***
- ***Second Offence – Written warning issued to student to go home to parents (phone call to be made before letter being sent home). Warning letter to be returned to school signed by parent, name recorded again.***
- ***Third Offence – short term (two week) suspension from using any Learning Technology facilities unless under direct supervision. Letter home to parents, name recorded again.***
- ***Fourth Offence – long term (one month) suspension from using any Learning Technology facilities unless under direct supervision, meeting with the parents.***

***Any subsequent offences would be dealt with under school-wide suspension procedures as outlined in the student code of conduct.***

***\*\* Please note that should a deliberate or particularly offensive act occur,***

***Level 1 – 3 may be bypassed.***

**All offences and actions taken will be reported (and recorded) to the Principal or Assistant Principal and the ICT Coordinator. Students will be made aware of these penalties on a regular basis in each classroom.**

The Acceptable Use Agreement also applies during school excursions, camps and extra-curricula activities. I acknowledge and agree to follow these rules. I understand that my access to the internet and mobile technology at school will be renegotiated if I do not act responsibly.

## **Part B - Student Agreement Aligned with School Values**

### **About the agreement:**

In signing this agreement your child will be agreeing to behave in a certain way online and to take appropriate action when and as required. The agreement also applies during school excursions, camps and extra-curricula activities. Elements of agreement are explained below.

### **Be a safe, responsible and ethical user whenever and wherever I use it.**

The School's Student Engagement/Wellbeing Policy outlines the values of the school and expected behaviours when students use the internet and digital technologies at school. Some portable technologies provided by the Department of Education and Training are available in students' homes.

### **Support others by being respectful in how I communicate with them and never write or participate in online bullying (this includes forwarding messages and supporting others in harmful, inappropriate or hurtful online behaviour).**

Being online can make students feel that they are anonymous and sometimes students may say things online that they would never say to someone's face. The web space or online chat environment that they use in leisure time might also have explicit language and they may feel they have to be part of it. Bullying online can take a number of forms from repeated messages to exclusion from social spaces. Students who forward on messages or participate in the exclusion may not see themselves as bullying. These actions also contribute to the hurt and distress of others.

### **Talk to a teacher if I feel uncomfortable or unsafe online or see others participating in unsafe, inappropriate or hurtful online behaviour.**

Incidents online often go unreported. Students have reported their reasons as embarrassment, a belief that online issues are theirs to solve as adults don't understand, a feeling that reporting it will make it worse and the most common reason given is a fear that they will lose access to their technology.

### **Students are advised to report an incident if:**

- they feel that the welfare of other students at the school is being threatened
- they come across sites which are not suitable for their school
- someone writes something they don't like, or makes them and their friends feel uncomfortable or asks them to provide information that they know is private
- they accidentally do something which is against the rules and responsibilities they have agreed to.

### **Seek to understand the terms and conditions of websites and online communities and be aware that content I upload or post is my digital footprint.**

Many websites/spaces have conditions of use, such as ownership of the content and the age of participants. For example: Children under 13 years of age are not permitted access to Facebook. When posting information online - A good rule is "Don't post what you wouldn't want anyone in your family, Principal or teacher to read."

### **Protect my privacy rights and those of other students by not giving out personal details including full names, telephone numbers, addresses and images.**

Students like to publish information about themselves and their friends in spaces like Instagram, Facebook and blogs. This can put them at risk of being approached, groomed or bullied online. To avoid this 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
- 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) so no full names should appear in reference to individuals in any image, movie or sound recording
- ALWAYS make the space private so that they can control who sees their space and can communicate with them
- understand the terms and conditions of any website or online community that they might join.

### **Use the internet at school for educational purposes and use the equipment properly**

It is important to realise that there is a time for fun and a time for work even on the internet. Students may often see the internet as 'free' however even just looking at a page on the internet incurs a download cost. By taking care with the equipment and thinking carefully about printing and downloading from the internet, students can save time, money and the environment. Staying on task will reduce the risk of inappropriate access and teach students strategies to use the internet or mobile technologies for their learning.

They will also have access to the rest of the internet. If your child is spending hours online 'doing their homework,' it may be that they are multitasking in many other applications, some of it study related and other interaction may be social.

**Use social networking sites for educational purposes and only as directed by teachers.**

Web 2.0 tools and social networking spaces allow students to be contributors to the web and to work collaboratively online with other students. Creating or contributing to blogs, wikis, digital stories and podcasts can all be legitimate educational activities which allow students to publish, share and inform others and be active contributors to the web. It is important for students to understand that working in a collaborative space as part of a learning task, has a very different purpose to using a social networking space to link up with friends in their own time.

**Abide by copyright procedures when using content on websites (ask permission to use images, text, audio and video and cite references where necessary).**

Music, information, images and games on the internet are owned by someone. The term copyright is a legal one and there are laws to enforce it. Not only is breaking copyright morally, ethically and legally wrong, it can introduce potential risks. By downloading a 'freebie' you can 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. Peer to peer sharing software like Limewire and Bit-torrent can sometimes share music and files illegally and make computers vulnerable.

**Think critically about other users' intellectual property and how I use content posted on the internet, not simply copy and paste information from websites.**

Not everything on the internet is true, accurate or unbiased. The school is working to teach digital literacy skills, which enable students to locate, evaluate and use information effectively on the internet. It is important that your child respects the Intellectual Property of people who contribute resources online. Students should use their own thoughts and language to express what they have learnt and avoid simply copying and pasting information from the internet.

In school settings, internet service providers set up filters to block out a lot of inappropriate content, but these filters are not always foolproof. Students who deliberately seek out inappropriate content or use technologies which bypass filters, will have their internet access reviewed and their parent/carers will be immediately informed.

Students must not:

- interfere with network security, the data of another user or attempt to log into the network with a user name or password of another student.
- use a virtual private network (VPN) application or similar technologies designed to circumvent the school's secure network
- reveal their password to anyone except the system administrator or classroom teachers.
- bring or download programs without permission, including games, to the school or run them on school computers.
- deliberately enter or remain in any site that has obscene language or offensive content (e.g. racist material or violent images).

Computer facilities are for the use of all students so due care should be taken at all times when using these resources. Students are responsible for everything done using their accounts and everything in their home directories. To this end, students need to keep their password secret and not gain access to other students' login details. The school connects all of the computers through a network. The introduction of unknown games or files could introduce viruses, etc and these put all school equipment and student work at risk.

**When using my digital device as a phone, I will:**

- keep the device turned off during school hours and only make or answer calls and messages outside of school times (8.45 am-3.15 pm)
- protect the privacy of others and never post or forward private information about another person
- seek permission from individuals involved before taking photos, recording sound or videoing them (including teachers)
- seek appropriate (written) permission from individuals involved before publishing or sending photos, recorded sound or video to anyone else or to any online space
- be respectful in the images I take or video I capture and never use these as a tool for bullying.

### **When using a digital device as a camera I will:**

- Only take photos and record sound or video when it is part of a class or lesson.
- Seek permission from individuals involved before taking photos, recording sound or videoing them (including teachers).
- Seek appropriate (written) permission from individuals involved before publishing or sending photos, recorded sound or video to anyone else or to any online space.
- Be respectful in the photos I take or video I capture and never use these as a tool for bullying.

The recording of images and sounds can breach students' rights under the Privacy Act. Sometimes students are reluctant to tell their peers that they don't want their image or voice recorded. The Privacy Act (2007) says that the posting and sharing of information online or in any other way requires consent.

This consent must be **fully informed, freely given, current** and **specific** in how the information will be presented and who it will be presented to. Schools are required to obtain signed authority for any work, images or information posted online. All citizens need to respect the rights of others to privacy and students are no exception. A sample consent form for requesting permission is available on the DEECD website. Consent can be withdrawn at anytime. (<http://www.education.vic.gov.au/management/elearningsupportservices/www/formstemp.htm#H2N10064>)

### **Family Information – Advice to support the safe and responsible use of digital technologies at home**

At school 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 and chat.

The term "space" is used here to describe a website that works like a community with live interaction and the capacity for your child to chat with others, personalise their space and share information. Each space has a purpose, audience and tool set including those around security and protection. The internet also provides access to websites with information, images videos for students to view. Not all content is presented as a space.

### **Key Discussion Questions for parents to ask**

At home we recommend you make some time to find out how your child is using the internet and iPad apps. Make some time to sit with them online and ask questions such as:

- What is it that is so enjoyable about the site or space you are using? What is the purpose of the site or space?
- How does it work? How do you set it up? What are the conditions of use?
- Who is else is sharing this space? Do you know them or did you 'meet' them online? How can you control who is in your space?
- 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?
- When would you tell an adult about an incident that has happened online? Who would you tell?
- When wouldn't you tell and why not?

### **Research shows that students are reluctant to report issues and put at risk their internet/phone access.**

Encourage your child to set their space to 'private' if they use a social networking site like Instagram or Facebook (they are then in control of who can contact them and access their information).

Ensure that all internet activities occur in a shared place – not your child's bedroom. Negotiate appropriate times for online activities and use of mobile phones. Consider the use of "safe search filters" freely available as settings on Google, Bing etc

### **Scenarios for teacher/parent/guardian/student discussion: What can you do?**

- Someone keeps messaging nasty and upsetting comments about you and your friends on your mobile phone.
- A person you met online asks you to give them your full name, phone number and suggests you meet. Is it different if they have been your "friend" for a long time?
- You are sent a message which has been forwarded by someone else. It has embarrassing comments/image about someone you know.
- A game online will only let you play it if you give your name, address, date of birth, etc.
- An online community asks you to sign up and allow the space to "Connect you to all your friends" It wants your email address and password to do this. It needs access to your address book.
- In an online space/chat someone suggests you all exclude/block a classmate.



- Your friend took a video of you and your friends ‘mucking around’ and posted it on a video hosting service like YouTube.
- You told your parent/guardian that you are doing homework for hours every night on the computer.
- Your friend has an online profile published (not set to private). You can see their personal details and photos. Other people you know are in the photos.
- A friend tells you about a great site where there is ‘free’ music or a game to download.

**Helpful parent links for cybersafety and cyberbullying (DEECD Bully Stoppers)**

- <http://www.education.vic.gov.au/Documents/about/programs/bullystoppers/smcyberbullying.pdf> (Parent Cyberbullying Advice Sheet from DEECD)
- <http://www.education.vic.gov.au/Documents/about/programs/bullystoppers/rtpdigitaltattoo.pdf> (Primary Digital Tattoo Advice Sheet from DEECD)
- <http://www.education.vic.gov.au/Documents/about/programs/bullystoppers/afnetiquette.pdf> (Netiquette Advice Sheet from DEECD)
- <http://www.education.vic.gov.au/Documents/about/programs/bullystoppers/smsocial.pdf> (Social Media Advice Sheet from DEECD)
- <http://www.education.vic.gov.au/Documents/about/programs/bullystoppers/sminappropriate.pdf> (Inappropriate Content Advice Sheet from DEECD)

If you have any concerns about this agreement contact the School Principal or the ICT Co-ordinator. For further support with online issues students can call Kids Helpline on 1800 55 1800. Parents/carers can call Parentline 132289 or visit <http://www.cybersmart.gov.au/report.aspx>

**Mt Eliza Primary School Student Acceptable Use Agreement**

**I have read the Mt Eliza Primary School Student Acceptable Use Agreement carefully and understand the significance of the conditions and agree to abide by these conditions. I understand that any breach of these conditions will result in internet and mobile technology access privileges being suspended or revoked.**

**Student Name:** .....

**Grade Level:** .....

**Student Signature:** .....

**Date:** .....

**Parent/Carer’s Name:** .....

**Parent/Carer’s Signature:** .....

**Date:** .....

**Evaluation:**

This policy will be reviewed on an annual basis: March/April 2020

School Council President:

Signature:

Date:

