

Thomastown West Primary School's motto is **Together Working on Pathways to Success.** At Thomastown West Primary School we want every child to achieve their full potential and we know that parents share this goal. We understand that students reach their full potential only when they are happy, healthy and safe, and that a positive school culture helps to engage students and support them in their learning. Our school acknowledges that digital learning is a 21st Century right of all our students. Digital technology has the power to transform the way students think and learn and give students a greater control over how, where and why they learn.

PURPOSE

To ensure that all students and members of our Thomastown West Primary 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 in years 3 to 6 and 1-to-3 iPads in the prep to 2 area.
- (b) expected student behaviour when using digital technologies such as the internet, social media, and digital devices (including computers, laptops, iPads, printers, camera)
- (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 their wellbeing or safety 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
- (e) the various Department policies on digital learning, including social media, that our school follows and implements when using digital technology
- (f) our school prioritises the safety of students whilst they are using digital technologies

SCOPE

This policy applies to all students and staff at Thomastown West Primary School Staff use of technology is also governed by the following Department policies:

- Acceptable Use Policy for ICT Resources
- Cybersafety and Responsible Use of Digital Technologies
- Digital Learning in Schools and
- Social Media Use to Support Student Learning.

Staff also follow our school's Acceptable Use Policy.

Staff, volunteers and school councillors also need to adhere to codes of conduct relevant to their respective roles. These codes include:

- Thomastown West Primary School Child Safe Policy and Child Safe Code of Conduct (available on our website https://www.thomwestps.vic.edu.au/articles/15 and at our school office)
- The Victorian Teaching Profession Code of Conduct (teaching staff)
- Code of Conduct for Victorian Sector Employees (staff)
- <u>Code of Conduct for Directors of Victorian Public Entities</u> (school councillors)



DEFINITIONS

Digital Technologies: For the purpose of this policy, "digital technologies" are defined as digital devices, tools, applications (apps) and systems that students and teachers use for learning and teaching; this includes Department-provided software and locally sourced devices, tools and systems.

POLICY

Vision for digital learning at our school

The use of digital technologies is a mandated component of the Victorian Curriculum F-10.

Safe and appropriate use of digital technologies, including the internet, apps, computers and tablets, can 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 learning that is interactive, collaborative, personalised, engaging and transformative. 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.

Thomastown West 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 interconnected 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.

Personal Devices at Thomastown West Primary School

At the time this policy has been written, Thomastown West Primary School does not permit students to bring personal devices. Our school currently provides all students with access to the following devices:

Prep: 1 to 3 iPads/laptops

Year 1/2: 1 to 3 iPads/laptops

• Year 3/4: 1 to 1 laptops

> Shared bank of 15 iPads

• Year 5/6: 1 to 1 laptops

Safe and appropriate use of digital technologies

Digital technologies, if not used appropriately, may present risks to users' safety or wellbeing. At Thomastown West Primary School, we are committed to educating all students to use digital technologies in ways that respect the dignity of ourselves and others and promote full flourishing for all, equipping students with the skills and knowledge to navigate the digital world.



At Thomastown West Primary School, we:

- use online sites and digital tools that support students' learning, and focus our use of digital technologies on being learning-centred
- use digital technologies in the classroom for specific purpose with targeted educational or developmental aims
- supervise and support students using digital technologies for their schoolwork
- effectively and responsively address any issues or incidents that have the potential to impact on the wellbeing of our students
- have programs in place to educate our students to be safe, responsible and discerning users
 of digital technologies, including complete Digital Licence in years 3 to 6, and following the
 eSmart curriculum.
- educate our students about digital issues such as privacy, intellectual property and copyright,
 and the importance of maintaining their own privacy and security online
- actively educate and remind students of our Student Wellbeing, Engagement and Inclusion
 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 technologies for their schoolwork
- use clear protocols and procedures to protect students working in online spaces, which
 includes reviewing the safety and appropriateness of online tools and communities and
 removing offensive content at the 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 at school to block access to inappropriate content
- refer suspected illegal online acts to the relevant law enforcement authority for investigation
- support parents and carers to understand the safe and responsible use of digital technologies and the strategies that can be implemented at home through regular updates in our newsletter, information sheets, website/school portal and information sessions.

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. This form is required to be signed at the time of the student enrolment.

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 E-Learning leader or a Principal Class member, immediately.

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.

Information on supervision arrangements for students engaging in digital learning activities is available in our Yard Duty and Supervision Policy.



Social media use

Our school follows the Department's policy on <u>Social Media Use to Support Learning</u> to ensure social media is used safely and appropriately in student learning and to ensure appropriate parent notification occurs or, where required, consent is sought. Where the student activity is visible to the public, it requires consent.

Thomastown West Primary School often uses social media platforms such as Facebook / Zoom to conduct school assemblies. Parents have the option to 'opt-out' if they have concerns about student participation.

Our school has established a live Facebook Page and a Class Dojo account. Assemblies and school events are sometimes streamed on this platform. As per our <u>Acceptable Use Policy</u> (Appendix A) Parents are welcome to contact the principal if they have any questions or concerns about students participating in this forum or withdraw their consent at any time.

In accordance with the Department's policy on social media, staff will not 'friend' or 'follow' a student on a personal social media account or accept a 'friend' request from a student using a personal social media account unless it is objectively appropriate, for example where the student is also a family member of the staff.

If a staff member of our school becomes aware that a student at the school is 'following' them on a personal social media account, Department policy requires the staff member to ask the student to 'unfollow' them, and to notify the school and/or parent or carer if the student does not do so.

Student behavioural expectations

When using digital technologies, students are expected to behave in a way that is consistent with Thomastown West Primary School's *Statement of Values, Student Engagement, Wellbeing and Inclusion 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), Thomastown West Primary School will institute a staged response, consistent with our student engagement and behaviour policies.

Responding to online incidents of inappropriate behaviour by students

*Refer to APPENDIX B for more details.

- Step 1: Identify concerns
- Step 2: Ensure safety
- Step 3: Take action
- > Step 4: Provide support

Staff record information on Compass in student chronicle.

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. Students understand that their access to digital technology at school may be renegotiated if they do not act responsibly. This includes:

- removal of network access privileges
- removal of email privileges
- removal of internet access privileges
- removal of printing privileges
- other consequences as outlined our Student Engagement, Wellbeing and Bullying Prevention
 policies. These policies can be found on our website and are also made available at our front
 office.



COMMUNICATION

This policy will be communicated to our school community in the following ways

- Available publicly on our school's website: https://www.thomwestps.vic.edu.au/page/101
- Included in staff induction and child safety training processes
- Discussed at staff briefings/meetings as required
- Included in our staff handbook/manual
- Discussed at parent information nights/sessions
- Included in Area newsletters so that it is easily accessible to parents, carers and students
- Included in transition and enrolment packs
- Included as annual reference in school newsletter
- Discussed at Class Meetings/Morning Circle.
- Made available in hard copy from school administration upon request

OTHER RESOURCES AND RELEVANT POLICIES

- TWPS Statement of Values
- TWPS Student Engagement, Wellbeing and Inclusion Policy
- TWPS Bullying Prevention Policy
- Digital Licence: https://www.digitallicence.com.au
- eSafety Commissioner: https://www.esafety.gov.au
- eSmart Framework: https://www.esmart.org.au/esmart-schools/

EVALUATION

• This policy will be reviewed as part of the Thomastown West Primary School four year policy review cycle.

Date Implemented	2016; 2020; 2022	
Author	Principal	
	Assistant Principal	
	eLearning Leader	
Approved By	School Council	
Date Reviewed	October 2016; November 2020, June 22	
Responsible for Review	Assistant Principal	
Review Date	10/06/2026	
References	Victorian Government Schools Policy Advisory Guide	



Appendix A

Acceptable Use Agreement for the Internet and Digital Technologies, 2022

Internet safety is an important issue for children. By the time young children arrive at school many are already online or using digital technologies. They visit their favourite websites, play games and use social media or apps.

At Thomastown West Primary School, we are committed to providing a learning environment that is rich in learning technologies to enable students to develop the skills required to be successful and responsible users of technology in our community. The school resources are used as educational tools and are used for research, communication, collaboration and publication. We use digital technologies such as the internet, intranet, computers and mobile devices as teaching and learning tools and acknowledge that they must be used responsibly.

Thomastown West Primary School recognises the need for students to be safe and responsible users of digital technologies. We believe that explicitly teaching students about safe and responsible online behaviours is essential and is best taught in partnership with parents/guardians. We request that parents/guardians work with us and encourage this behaviour at home.

Although the school has steps in place to reduce the risks accompanying internet and digital technologies use, students may encounter digital information resources that have not been screened by educators for use by children. Therefore, parental/guardian approval is required before students access the school resources.

At our school we:

- support the rights of all members of the school community to engage in and promote a safe, inclusive and supportive learning environment.
- use our school's core values of respect, responsibility, tolerance and excellence to educate our students to be safe and responsible users of digital technologies and as the basis for discussions about how we treat others in an online environment.
- have policies that outline the values of the school and about the expected standards of student behaviour, including actions and consequences for inappropriate behaviour.
- educate our students to be safe and responsible users of digital technologies.
- raise our students' awareness of issues such as online privacy and intellectual property including copyright.
- provide supervision when using digital technologies for learning.
- provide a filtered internet service but acknowledge that full protection from inappropriate content can never be guaranteed.
- respond to issues or incidents that have the potential to impact on the wellbeing of our students.
- know that some online activities are illegal and as such we are required to report this to the police.
- provide parents/guardians with a copy of this agreement.
- support parents/guardians to understand the importance of safe and responsible use of digital technologies, the potential issues that surround their use and strategies that they can implement at home



Students' Safe and Responsible Behaviour

When I use digital technologies (e.g. Internet, Intranet, computers, and mobile devices such as iPads, cameras, iPods etc) at school I agree to:

Communicate respectfully by thinking and checking that what I write, post, say or do is polite and respectful. This means:

- never sending mean or bullying messages or passing them on, as this makes me part of the bullying.
- not using actions online to be mean to others. (This can include 'leaving someone out' to make them feel bad).
- not copying someone else's work, ideas, pictures, videos or music from the internet and presenting them as my own.

Protect personal information by being aware that my full name, photo, birthday, address and phone number is personal information and not to be shared online. This means:

- protecting my friends' information in the same way.
- protecting my passwords and not sharing them with others.
- only joining a space online with my parent or teacher's guidance and permission.
- never answering questions online that ask for my personal information.

Look after myself and others by thinking about what I share online. This means:

- I agree to follow all teacher instruction and live by our school values communicating in an online environment.
- never sharing my friend's full names, birthdays, school names, addresses and phone numbers because this is their personal information.
- speaking to a trusted adult if I see something that makes me feel upset or if I need help.
- speaking to a trusted adult if someone is unkind to me.
- speaking to a trusted adult if I know someone else is upset or scared.
- stopping to think about what I post or share online.
- never responding to online bullying, instead take a screenshot, close the app or device and make a time to show your teacher or Principal.
- using spaces or sites that are right for my age.
- not deliberately searching for something inappropriate or violent.
- either turning off the screen or using the back button if I see something I don't like and tell a trusted adult.
- being careful with the equipment I use and tell a trusted adult if any equipment is damaged.
- not interfering with the network, the work or data of another user or attempt to log into the network with a username or password that is not my own.
- asking others before I use their photo or 'voice' in my own work.
- not arranging to meet anyone I have contacted online.
- If using an USB memory stick, SD card, or the 'cloud', it will only be used to retrieve or transfer the files related to my school work. It is not acceptable to copy, download or put my own software or items unrelated to my school work from the Internet on the Netbooks as this may cause a virus or interfere with the *DET Edustar* image.
- that I understand that system administrators and teachers may access my files and delete files at any time to conform to storage requirements or the terms of the Acceptable Use Agreement.



Student Commitment

This Acceptable Use Agreement applies to digital technologies, social media tools and learning environments established by our school or accessed using school owned networks or systems, including (although are not limited to):

- School owned ICT devices (e.g. iPads, laptops, netbooks, printers, scanners, 3D printer)
- Email, instant messaging and software that includes 'Chat'. (e.g. Minecraft)
- Internet and Intranet
- Social networking sites (e.g. Edmodo, Google Classrooms, Dojo)
- Video and photo sharing websites (e.g. Picasa, Vimeo, YouTube)
- Blogs
- Micro-blogs (e.g. Twitter)
- Forums, discussion boards and groups (e.g. Google groups, Whirlpool)
- Wikis (e.g. Wikipedia, Wikispaces)
- Vodcasts and podcasts
- Video conferences and web conferences. (Eg. Webex, Zoom)
- Live streaming (eg. Facebook live)

This Acceptable Use Agreement also applies during school excursions, camps, extra-curricular activities and when using online school spaces at home. I acknowledge and agree to follow these rules. I understand that my access to digital technology at school will be renegotiated if I do not act responsibly.

I have read the Acceptable Use Agreement with my parents carefully and understand the significance of the conditions and agree to follow all of these rules. I understand that if I break these rules, I will not be allowed to use technology for a negotiated period of time.

Student Name:	1 mitted	Room:	
	and & submit		
	Signed Town 1		
Student Signature: _	in Term	Date:	
•			



Annual Consent Form and Collection Notice

I have read through and discussed the responsible use of the digital technologies with my child and understand that if my child does not follow these behaviours, they will not be allowed to access technology at school for a negotiated period of time. I agree to:

- allow my child to use the internet and digital technologies at school
- allow my child being photographed/filmed within the context of the regular school program.
- allow photographs/film to be used within the school for publication within the school (i.e. newsletter, school internal network, classroom displays or school displays)
- allow photographs/film to be used on school internet sites or school social media accounts operated by the School Principal (such as Facebook, Twitter or Instagram) with identification of the first name only
- allow photographs to be released to the media such as local newspapers
- allow publication of my child's work and first name on school and internet sites
- allow my child to participate in live stream digital platform ie. Facebook for school assembly/ community news etc
- allow my child to watch **PG** movies
- allow my child to sign up for websites that are deemed appropriate by my child's teacher.
- cover the repair cost of the device my child is using, if it is damaged by their inappropriate behaviour and not following the school values. (This will not exceed \$100).

I will contact the school if there is anything here that I do not understand. If there is a situation which concerns me, I will contact the school. I understand that I can also receive support from the CyberSmart website www.cybersmart.gov.au/report.aspx or Parent Helpline 132 289.

Parent/Guardian Signature: ₋	
Date: / / 2022	
Student name:	
Room:	



Appendix B



Responding to online incidents affecting students

Step 1: Identify concerns

An online incident can include:

- cyberbullying
- · threats of violence and/or intimidation
- · image-based abuse and/or sextortion
- exposure to graphic or pornographic images
- viral hoaxes
- other online breaches of the school's Bullying Prevention and Response Policy, Cybersafety or Student Engagement Policy.

Has a student's actions affected another student?

A student may have engaged in behaviour online that may cause psychological or emotional harm to another student.

Have a student's actions put themselves at risk of harm?

A student may have engaged in behaviour online that may cause psychological or emotional harm to themselves (such as sending explicit images).

Does the incident involve criminal behaviour?

A student may have engaged in behaviour online that could be deemed as criminal activity.

Step 2: Ensure Safety

If an online incident is suspected or identified, it is important to first make sure the student/s involved are in a safe environment. Respond to the immediate needs of students, staff and any other parties and contact emergency services on 000 if required.

Inquire into the incident

This may include discussions with staff and students who have been directly or indirectly involved the incident.

When talking to student(s) remember to:

- Stay calm and listen
- Reassure the student(s) that they will be supported and that the issue can be resolved
- Depending on the incident, ask the student(s) how they would like to resolve the issue
- Refer to relevant school policies and ensure to record the incident
- Seek advice and input from the wellbeing team or other members of school leadership as needed about addressing the issue
- Refer the incident to the wellbeing team, year level coordinator or other member of school leadership if the incident is complex, ongoing, involves numerous students, you are concerned a criminal offense may have occurred and/or you are concerned about the safety and wellbeing of students or others who may be involved.





Step 3: Take action

The incident, student(s) involved and whether it has been referred will determine next steps. In some instances, classroom teachers may feel confident and comfortable addressing an incident. In other instances, further action may be required as per your school's Bullying Prevention and Response Policy, Cybersafety or Student engagement policy. Follow appropriate processes and procedures.

If a criminal offence may have occurred, contact Victoria Police.

A member of the school's leadership team is often best placed to lead contact with the police.

Seek advice from the police if unsure whether an incident is a criminal offence. Depending on the incident, the police

may also provide advice about contacting the parents of all students involved in the incident.

Incident Support and Operations Centre (ISOC)

The incident may need to be reported to ISOC.

Incidents rated as Extreme, High, or Medium must be **reported to ISOC for immediate advice and coordination of Area-based supports**; and recorded by the school on CASES21 or equivalent records management system

Contact ISOC on 1800 126 126 for further advice about incident ratings.

Step 4: Provide Support

Provide support as needed to all students and staff who were involved in or witness to the incident. This could include:

- Parent/carer meetings
- School based wellbeing support
- Referral to external supports
- Ongoing monitoring and other targeted strategies
- Development of a Behaviour Support Plan
- Education on the acceptable use of technology

Contact your local regional office for further advice if required

Recording information

Remember to:

- Keep records of the incident (such as screenshots where appropriate, notes from the interviews)
- Record the process taken to resolve the incident (such as steps taken to remove content, mediation attempts).
- Be aware that there may be issues around the collection of images of people under 18 who
 are victims of sexual abuse, in a sexual pose or activity or who is naked and that may be
 offensive. It is illegal to possess or distribute this material unless you possess it in good
 faith, in the course of your official duties and to assist a police investigation.





If you are concerned that a mobile phone, laptop, other device or document may contain
child abuse material, seek advice from Victoria Police and follow any directions they give
you about confiscating, handling, possessing or dealing with the device and its contents.
Record carefully the advice from Victoria Police and the steps taken after receiving that
advice.

For more information on ways to record the incident, or to support a student to do so, see the eSafety Commissioner's <u>Collecting Evidence</u> page.

Key contacts and additional resources

ISOC

Contact ISOC to report incidents or for advice and coordination of Area-based supports on 1800 126 126

More information on mandatory reporting and the Severity Rating Decision-making Matrix is available on the Department's Policy and Advisory Library.

Regional Office contacts

- North Eastern Victoria
- 1300 333 231 nevr@education.vic.gov.au
- North Western Victoria
- 1300 338 691 nwvr@education.vic.gov.au
- South Eastern Victoria
- 1300 338 738 sevr@education.vic.gov.au
- South Western Victoria
- 1300 333 232 swvr@education.vic.gov.au

Other resources

Bully Stoppers

For more information about bullying and cybersafety, search for Bully Stoppers.

PROTECT

 For more information on Child Safe Standards and identifying and responding to all forms of abuse in Victorian Schools, search for PROTECT.

The eSafety Commissioner

 The office provides a range of up-to-date information and resources, coupled with a complaints system to assist children who experience serious cyberbullying and imagebased abuse. See: www.esafety.gov.au

Kids Helpline: 1800 55 1800

Beyond Blue: 1300 22 4636

headspace: headspace.org.au

Reach out: au.reachout.com