Manurewa Central School

Digital Technologies and Cybersafety Policy

RATIONALE:

Manurewa Central School supports the implementation and use of digital technologies in teaching and learning programmes with the New Zealand Digital Curriculum guiding its use and implementation. Accessing the internet is restricted according to the school's firewalls. The policy applies to every member of the school community authorised to use the digital technology equipment, including staff, students, volunteers, trainees, contractors, special visitors, and board members. It applies to digital devices/equipment owned or leased by the school and also those privately owned. It applies whether the digital technology equipment is used at the school, or any other location for a school based activity. This includes off-site access to the school network.

Digital technology equipment includes, but is not limited to: computers, storage devices, cameras, mobile phones, gaming consoles, video/audio devices, smart watches etc., whether owned by the school, or privately.

PURPOSE:

The board recognises Digital technology has an increasing role in teaching and learning, in running our workplaces, and in our daily lives. We value our internet facilities and ICT digital technology equipment and the benefits they bring us in learning outcomes and the effective operation of the school.

We actively encourage our students to be competent and confident in the use of digital technology; and aware of and able to manage the challenges and issues that go with it. These issues include safety of themselves and others, privacy, copyright, and protection of digital devices and equipment.

Our vision for tamariki who are good digital citizens is someone who;

is inspired to **'dream big'**

- Is a confident and capable user of ICT

have the potential to **shape their future**

- Will use ICT for learning as well as other activities
- Will be able to speak the language of digital technologies

believes in themselves and take **pride** in their achievements

- Will help others to become better digital citizens
- Will always respect people's privacy and freedom of speech online
- Will be honest and fair in all of their actions using ICT

learn without limits

- Will always use ICT to communicate with others in positive ways
- Will think carefully about whether the information they see online is true
- Understands that they may experience problems when using technology but can deal with them

GUIDELINES:

In keeping with our Health, Safety, and Welfare Policy, we follow procedures to guide our use of the internet, mobile phones, and other digital devices and equipment. We maintain a cybersafe school environment by:

- educating students and the school community about the safe and responsible use of information and communication technologies
- ensuring that systems are effectively maintained, secure, and filtered when necessary. Students are not able to 'surf the web' at any time.
- using NetSafe resources
- allowing for professional development and training for staff
- setting and sharing clear guidelines about acceptable and unacceptable use of the technology including use of Generative Technology (AI), and monitoring these guidelines
- following clear guidelines about publishing student information online
- having a clear process for dealing with breaches of the policy or agreements, including any incidents of cyberbullying
- following guidelines for the surrender and retention of digital devices
- ensuring that all members of the school community understand the policy, and commit to it by signing the appropriate Use Agreement which outlines requirements and expectations
- reviewing use agreements annually.

The school maintains the right to monitor, access, and review digital technology use, including email use; and to audit at any time material on the school's equipment. The school may also ask to audit privately owned digital technology devices/equipment used on the school site or at any school related activity.

The school upholds its information privacy principles with the guidelines in the Privacy policy.

The safety of students is of paramount concern. Any apparent breach of cybersafety will be taken seriously. The response to individual incidents involving staff will follow the school's procedures which detail how to investigate a formal complaint or serious allegation. In serious incidents, advice will be sought from an appropriate source, such as NetSafe, Te Whakarōputanga Kaitiaki Kura o Aotearoa – New Zealand School Boards Association (formerly NZSTA), and/or a lawyer with specialist knowledge in this area. There will be special attention paid to the need for specific procedures regarding the gathering of evidence in potentially serious cases. If illegal material or activities are suspected, the matter may need to be reported to the relevant law enforcement agency.

Cyberbullying Procedures

Manurewa Central School has strategies in place to prevent cyberbullying where possible and respond to it if it occurs.

Prevention

- Ensure a whole-school focus on an inclusive and supportive environment.
- Promote **good digital citizenship** both inside and outside the classroom. For example:
    - Teach students about safe and responsible technology use
    - Develop class contracts about appropriate use of technology, including, how, and when, mobile devices may be used at school
    - Have students, staff, and/or parents sign ICT digital technology use agreements
    - Provide ongoing education and advice to parents and whānau about how to protect their children online, and inform parents and whānau about any cyberbullying incidents at the school.
- Ensure teachers understand the surrender and retention of digital devices guidelines.
- Engage teachers in ongoing professional development about technology in learning environments including the use of AI.
- Provide guidance to students about how to stay safe online. For example:
    - Activate privacy settings on social media sites
    - Only give personal information to people they know and trust
    - Use available online safety options (e.g. website blockers and email/spam filters)
    - Avoid sharing images of themselves they wouldn't want distributed further
    - Know how to contact a service provider to report abuse or problems.
    - Understand the challenges and limitations of AI.

Response

- Get offensive or inappropriate online material removed if possible:
    - Ask the person responsible to take down the offending website, page, or information
    - Request the service provider or website owner to remove the page or information
    - Seek further advice from NetSafe.
- Emphasise to students that they can talk to an adult they trust (parent, teacher, etc.) if they feel bullied, without worrying about negative consequences (such as having their phone taken away).
- Report inappropriate text messages to the student's service provider, or support the student in doing so.
- Use "report abuse" buttons or other feedback methods on websites to report abuse or bullying.
- Use the behaviour management policy to deal with incidents of cyberbullying

<u>Responding to Digital Incidents</u>

At Manurewa Central School we have clear guidelines about acceptable and unacceptable use of technology; and students, caregivers, and parents sign use agreements. We take any breach of cybersafety seriously and respond as appropriate.

A major digital incident such as the posting of highly personal information or a graphic photo/video online can have a significant impact on students and staff. The school has the authority and responsibility to act, even when the incident takes place outside of school.

If damaging content has been posted online, the school acts to minimise student/staff distress and ensure their safety. We follow our policy for the surrender and retention of digital devices, and we apply our behaviour policy in cases of unacceptable student behaviour.

In response to a digital incident, the school will:

- gather the facts to determine what has happened and who is involved
- support the students/staff involved
- determine the nature of the content (is it illegal, threatening or intimidating, objectionable, or does it breach privacy?)
- seek advice from other organisations if necessary, e.g. Netsafe, the Ministry of Education's traumatic incident team, and/or the police
- contact other relevant parties, e.g. senior staff, the board of trustees, pastoral staff, or parents/caregivers
- determine how/when to release information to the wider community and the media
- record full details of the incident.

After the incident is resolved, the school continues to monitor the well-being of the affected students/staff and provides support if needed. The school holds a debrief to assess management of the incident, and how well the cybersafety guidelines were implemented.

Surrender and Retention of Digital Devices

The school fosters a positive culture of safe and responsible use of digital devices through the Digital Technology and Cybersafety policy and use agreements. We encourage students to be confident, capable, and responsible in their use of digital technology. Inappropriate use is dealt with as appropriate through the behaviour management plan and or surrender and retention guidelines.

Surrender and retention applies to items and devices that are:

- likely to endanger safety
- Depending on the circumstances, this category could include images, social media posts, texts, audio, video, etc.
- likely to detrimentally affect the learning environment
- This is anything that disrupts the flow of teaching and learning. It may include any item or device, that while harmless in itself, is used in an annoying or attention seeking (and therefore disruptive) way.
- harmful
- Any item deemed to pose an immediate threat to a person's physical or emotional safety is harmful. This is the only category that may warrant a search.

At all times, staff members must use their judgement about whether an item or device fits into these categories, considering the circumstances.

The focus must be on the inappropriate behaviour, i.e., causing disruption in the class, or compromising the safety of an individual, rather than on the technology itself. The school's cybersafety agreements and behaviour management plans set out what is acceptable and the consequences of inappropriate behaviour. Incidents involving digital devices are

managed with due respect for the student's safety and privacy, and the integrity of the device and contents.

In the case of disruption of the learning environment, teachers and authorised staff can ask the student to show them the item, and/or to delete it; may ask the student to put the device away, or surrender the device to be retained for a reasonable period. If the student refuses to cooperate, they are managed through the school's behaviour management plan. Due to the nature of digital technology, items can be quickly and easily shared, and difficult to delete. Teachers can ask the student about the source of the item and whether it has been shared, etc., as this will help determine the action taken.

The same applies in the case of an item that is likely to endanger safety, and there are extra factors to consider, such as the emotional impact on the people affected; whether the item has been, or could be, shared or stored; the nature of the item, and maturity and age of the students involved. The school may contact NetSafe for advice, and will contact the police if a criminal offence is suspected, for example, drug involvement, threats to kill or assault, etc.

Staff cannot ask students to download or reveal what is on another digital device, such as a social media site, or storage system. Staff cannot search the student's device contents or online accounts, or ask for the student's password for the device.

Staff cannot **search** a device. The New Zealand Police have the ability and authority to search a digital device and must be contacted if a search is deemed necessary.

If a criminal offence has occurred or is suspected, the device is passed to the New Zealand Police as soon as possible.

Retention of digital devices

- Retained digital devices are stored securely and appropriately.
- If it has the capability, the device is turned off and locked when it is given by the student.
- A record is kept including details of the incident, and the device.
- The device is returned at the end of the retention period to the student, or their parent/caregiver, as appropriate.

RELATED POLICIES:

Health, Safety and Welfare Policy
Surrender, Retention and Searches Policy
Complaints Policy
Behaviour Management Policy
Privacy Policy
Digital Technology User Agreements/Pledges/Consents

Date reviewed:	11 November 2024	Next Review: March 2026	
PM BOT:		Principal:	