TECHNOLOGY POLICY

PURPOSE

Newmark Primary (the school) is committed to the safe and acceptable use of technology. The school recognises the important role that technology plays in the world, and the need for students to be digitally literate in order to thrive in the world. The school uses technology purposefully to learn, build, communicate and create.

The purpose of this policy is to provide students, staff and parents/carers with clarity as to the acceptable use of technology in the school.

PRINCIPLES

- The school believes that it has a responsibility, in partnership with parents/carers, to ensure students are safe in all environments (including both physical and digital).
- The school believes that the same values and behaviour that govern respectful and inclusive interactions in the physical environment, must also govern interactions in the digital environment.
- The school believes that students must be digitally literate in order to thrive in the world.
- The school has zero tolerance for any form of bullying and harassment, in both the physical and digital environments.
- The school, in discharging its duty of care, understands that it has a responsibility to enable students to flourish in relation to their emotional, social, mental and physical health.

AIMS

- To set out the school's approach to the purposeful use of technology
- To support the school and its staff, parents/carers and students in understanding what is acceptable use of technology

LEGAL AND REGULATORY BASIS FOR COMPLIANCE

- Duty of Care
- Education and Training Reform Act 2006 (Vic.)
- Education and Training Reform Regulations (2017)
- Child Wellbeing and Safety Amendment (Child Safe Standards) Bill 2015 (Vic.)
- Ministerial Order 1359 January 2022 (Vic.)

KEY DEFINITIONS

Duty of care: The school has a duty of care to ensure the safety and wellbeing of students. In discharging this duty, the principal, teachers and other school staff are held to a high standard of care in relation to students. The duty requires principals and teachers to take all reasonable steps to reduce the risk of harm to students, including the implementation of strategies to

create a culture of respect and inclusion. The duty is non-delegable, meaning that it cannot be assigned to another party.

Devices: The school currently uses a variety of devices, including but not limited to:

- **iPads** (for students)
- **Laptops** (for staff)
- **Desktops** (for staff)
- **Smart Boards**

Platforms: There are a few key platforms that the school uses, including:

- **Storypark** - used to communicate with families
- **Slack** - used to communicate with staff
- **Zoom** - used to connect with remote communities and individuals
- **G Suite** (Google Apps For Education) - used to collaborate and store information
- **PC Schools** - used as a data management system

Apps: The school uses a range of Apps that are age appropriate and beneficial to learning, communicating and creating.

Other Digital Technology Resources: The school uses a range of digital technology resources as part of the teaching and learning program to teach skills such as robotics, coding and circuitry.

Firewall Protection: Firewall refers to a network device which blocks certain kinds of network traffic, forming a barrier between a trusted and an untrusted network.

Technology Protocols: Protocols are used to guide the use of devices in the school by staff and students.

SCOPE

The application of the policy is relevant to staff, students and parents/carers.

ROLES AND RESPONSIBILITIES

The **school board** is responsible for:

- reviewing and endorsing the Technology Policy.

The **principal** is responsible for:

- overseeing the implementation of the Technology Policy;
- ensuring all staff understand their duty of care, and responsibilities to ensure acceptable use of technology in the school;
- supporting staff in 'Response to Incidents' when protocols are breached by students;
- overseeing performance management processes when protocols are breached by staff;
- overseeing platform administration (allocating and removing platform access); and
- overseeing and monitoring the risk management plan.

The **Business Manager** is responsible for:

- managing external service providers to purchase and maintain equipment and networks;

- managing equipment and network repairs and upgrades as required;
- maintaining the security of devices and networks, including appropriate web filtering settings;
- securing the most cost efficient arrangement for devices selected by the school; and
- liaising with third party vendors.

The **staff** are responsible for:

- raising awareness of safe use of technology, including cybersafety;
- ensuring all platforms and apps on the device are age-appropriate and safe;
- ensuring all security and privacy settings are appropriately adjusted prior to students using a platform, app or device;
- monitoring the use of devices to ensure students are using them in an acceptable way;
- checking the history of devices to ensure students are using them in an acceptable way;
- responding to incidents when devices have not been used in an acceptable way;
- ensuring all devices are handled with care, and putting appropriate procedures in place, so that damage to devices is avoided, and reporting damaged devices to the Business Manager;
- ensuring devices are locked away, and keys are hidden at the end of every school day; and
- abiding by the protocols for staff.

The **students** are responsible for:

- taking care of their devices and using them appropriately;
- locking away devices at the end of the day;
- ensuring devices are charging overnight, ready to be used the following day;
- abiding by the protocols for children; and
- reporting misuse of a device to a staff member immediately.

PROCEDURES

In order to ensure students are safe, and devices are cared for appropriately, the school implements the following procedures.

FIREWALL PROTECTION

All devices used by students have been set up with a Firewall to prevent students from accessing, and being exposed to inappropriate sites, information or images.

On rare occasions where students do encounter inappropriate sites, information or images, the following steps must be taken:

1. Students immediately tell the teacher, and show them the site;
2. The teacher reports this to a member of the leadership team; then
3. A member of the leadership team consults with the appropriate bodies to investigate the reason for this incident, in an effort to ensure it does not happen again.

RISK MANAGEMENT PLAN

In order to minimise potential risk to students when using technology, the school has developed a Risk Management Plan (RMP). This plan will be monitored and reviewed by the principal and the tech team.

Reviews of this RMP will be conducted at least annually, and in circumstances where unexpected incidents occur.

SECURITY/PRIVACY SETTINGS

Prior to a platform, app or device being used by students, staff will ensure that all the appropriate security and privacy settings are in place and working. The set up must be checked and approved by the member of the tech team prior to students using it.

In cases where there is uncertainty about the security and privacy of a platform, app or device the school will prohibit the use of it.

Students will be taught about the safest way to use personal social media platforms to raise an awareness of the potential dangers (even though the students do not use these while at school, it is important that they are aware of how to engage safely in forums such as online games, use of apps, and social media platforms). This will include ensuring all appropriate security and privacy settings are switched on.

PASSWORDS

Staff devices: Staff must have their own private password to their school devices (laptops and iPads) and ensure that auto-lock settings are enabled. These passwords must not be shared at any time with students, as these devices do not have firewall protection, and hold sensitive information.

Student devices: The school's preference is that student iPads do not have an access password, as they are shared devices and need to be accessed by different staff members as part of the teaching and learning program. If there is a reason that a staff member believes it necessary to use a password, they must use: 4466 for all devices.

Student platforms and apps: At times it will be necessary to use personal passwords for student platforms and apps. This is only the case when personal student data is held in these places (eg reading levels, achievement with maths modules etc). In these cases, the following steps will be followed:

- Students will be given their password details, and shown a private place to keep the information (eg in a personal workbook). Passwords will not be displayed for others to see in the studio.
- At times, password details will be emailed to parents/carers if a platform or app is to be used at home.
- Staff will keep all student passwords in a common, secure digital space, that can only be accessed by designated staff members (eg. Google Shared Drive > Google Sheet).
- Students should not change any allocated passwords.

To ensure the school's passwords are secure, the school uses a password management system that is only accessible by selected members of the leadership team. Passwords are not to be changed by other staff members, however requests can be made for a password to be changed by emailing: tech@newmark.vic.edu.au

Passwords should not be written down.

STORAGE OF DEVICES

The school provides lockable units for all student devices to be stored in when not in use during the school day, and overnight. Student devices must not be left out in the open when not in use, this included during recess and lunch breaks, and when the students are participating in another lesson (eg. PE, Art). Prior to these sessions, all devices must be locked away.

It is the responsibility of staff and students to:

- ensure devices are in the lockable units when not being used during the day, and overnight;
- ensure lockable units are locked both during the day and overnight, and that the key is hidden; and
- ensure that devices are plugged in to charge when in the lockable units so that they are ready to use as part of the teaching and learning program.

Staff devices must be put out of view, and in a secure place when not being used. This includes not leaving devices in common staff spaces, and not leaving devices unattended and visible in learning studios. Examples of appropriate places to leave laptops while not in use are:

- in a cupboard;
- in the lockable unit with the student devices (this is recommended if the device is going to be left unattended for a long period of time during the school day eg. if a staff member is attending sport for the morning); or
- in a personal backpack or bag.

APPROVAL PROCESS

At times staff find new platforms, web-based programs and apps to use with students. It is important that all the digital tools and resources used at the school are safe, age appropriate and align with the school's philosophy.

For this reason, the following steps must be followed by staff to gain approval prior to securing a subscription or deploying an app:

1. Send the following information via the Slack #technology channel:
    a. Name of the resource
    b. Link to the resource
    c. Number required (if applicable eg. how many apps)
    d. Total cost of the resource (including if it is a one-off or annual cost etc)
    e. Reason for wanting to obtain the resource (eg. how it will be used)

2. The tech team will review the requests once a week, and will either ask follow-up questions, or approve/deny the request. If the request is denied, the tech team will provide a reason.

3. If the resource is approved, the tech team will support the deployment of the resources to the appropriate devices.

EMAILS

All school emails (both staff or students) are to only be used for school purposes.

In order to encourage a culture of transparency, all staff emails must bcc the appropriate group (eg. current-families@). This will ensure that all emails are appropriately archived into groups, and can be easily accessed at any time. It will also ensure that the appropriate staff members can view the emails, and are aware of communications that have occurred.

Students are allocated personal email addresses, as this allows access to key platforms used by the school. However it is important to note that students do not begin to use school emails as a mode for communication until they are in the upper primary school years. When school emails are used, it is the responsibility of the staff to monitor and check that all emails are for school purposes and are appropriate.

INTERNET USE

All student devices have chrome as a search function, however this function is not used independently by students until they are in Year 2. At this time, staff are responsible for teaching safe use of search functions, and for setting expectations of safe use of the internet.

MOBILE PHONES and SMART WATCHES

All communications between student and parent/carers during regular school hours, outings and camps must be facilitated by the school staff. This enables the school to monitor and appropriately respond to situations that occur, and in so doing, fulfil its duty or care for students.

Students are not permitted to contact parents or any other person via a personal device, nor are parents/carers to contact students via a personal device during regular school hours (including recess and lunch time), outings and camps.

If parents/carers need to communicate with a student during these times, they can call 03 8560 4466 or email hello@newmark.vic.edu.au.

If a student needs to communicate with a parent/carer during these times, they can:

- talk to a teacher to determine if it is necessary to speak to a parent/carer; and
- if it is necessary to contact a parent/carer, the teacher will find the most appropriate way for this to be done (e.g. ask the Front Office Manager to call, send an email etc).

In order to ensure that these appropriate and safe communication channels are used, the following process will be used:

MOBILE PHONES

- Upon arrival at school students must hand in their mobile phones.
- The mobile phones will be stored in a secure place for the duration of school day, outing or camp.
- The mobile phones will be returned to students at the end of the school day, outing or camp when they are leaving to go home.

SMARTWATCHES

- Upon arrival at school students must turn off all smartwatch functions that allow access to the internet, calls or messages.

- Once students have been released by supervising staff at the end of the school day, outing or camp they can turn on the smartwatch functions.

Students that do not abide by the above processes will be asked to not bring devices on school premises.

RESPONSE TO INCIDENTS

In cases where protocols are breached, the school will be guided by advice provided in the eSafety Toolkit for Schools (eSafety Commissioner) as serious cases can require the involvement of outside organisations (eg. the police).

If a breach occurs, the school will follow these steps to resolve the conflict:

1. The school will use the 'Online Incident Assessment Tool' which is part of the eSafety Toolkit for Schools, to assess the seriousness of the incident. https://www.esafety.gov.au/educators/toolkit-schools/respond
2. If the incident is considered 'mild' or 'moderate', the school's internal process will most likely be used to guide the response (see Wellbeing Policy).
3. If the incident is considered 'serious' or 'severe' the school will most likely use the process outlined in the eSafety Toolkit for Schools. As this can include the involvement of outside organisations, the school believes it is best to be guided by experts in its response.

In cases where a staff member breaches the protocols, they may be guided through the appropriate 'performance management' processes.

RELATED POLICIES

- Wellbeing policy
- Bullying Prevention policy
- Child Safety policy
- Reporting Obligations policy
- Child Safe Code of Conduct

SUPPORTING RESOURCES

- Technology Protocols
- eSafety Commissioner Resources https://www.esafety.gov.au/educators/toolkit-schools

POLICY REVIEW

The school board and principal will review the Technology Policy every two years, or following a major incident.

ENDORSEMENT

Updated date	January 2023
Endorsed by	School Board
Endorsed on	April 2023

TECHNOLOGY PROTOCOLS FOR CHILDREN

Use the device that has been assigned to you.

Set the background using the wallpaper on the device.

Use the devices for school-related learning, creating and communicating.

Check with your teacher before sending a message.

Use kind words when communicating with others.

Turn the airdrop and airplay off when you are not using them.

Use your device at a table or on the lounge (not on the floor).

Walk with your device, holding it with two hands and leaving the cover closed until you are sitting down.

Sit so others can see the screen of your device.

Check with a teacher before printing.

Put your device away when you have finished using it.

Make sure all the devices are away before you leave the learning studio.

Plug the devices in at the end of the day and lock the cabinets.

Let a teacher know straight away if something inappropriate pops up on your screen, or if a device is being used inappropriately.

TECHNOLOGY PROTOCOLS FOR STAFF

Make sure children in your care understand and abide by the 'Technology Protocols for Children'.

Monitor and check the use of devices by children in your care.

Establish systems and routines that help children take care of their devices.

Make sure all programs and apps are age appropriate on the devices.

Check all sites prior to sharing them with children.

Make sure security settings are checked and on.

Make sure children are supervised adequately when using devices.

Make sure children use the device that is allocated to them.

Follow the appropriate procedures if an incident occurs.

Put devices away during wet day / sweat day recess and lunch breaks.

Make sure devices are locked away at the end of each day and that the keys are out of sight.

Set a personal password to secure your own device and don't share it.

Use your device at a table or on a lounge (not on the floor).

Close your device when you are not working on it.

Put your device away when you are not working on it, out of sight.

Return your device when departing with the password, without deleting any files, content or emails.