Maryborough Education Centre

Digital Technologies (Internet, Social Media and Digital Devices) Policy

PURPOSE

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

(a) Maryborough Education Centre's (MEC) commitment to providing students with the opportunity to benefit from digital technologies to support and enhance learning and development at school including the 1-to-1 personal device program

(b) the expected student behaviour when using digital technologies including the internet, social media, and digital devices (including computers, laptops, tablets, phones)

(c) MEC'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) MEC's policies and procedures for responding to inappropriate student behaviour on digital technologies and the internet.

SCOPE

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

Detailed information for each area of ICT use can be found in the following documents:

- **Appendix A**: MEC Bring Your Own Specified Device (BYOSD) Specifications
- **Appendix B:** Information for Parents and Students
- **Appendix C:** Digital Technologies Behaviour Management Process
- **Appendix D:** MEC Acceptable Use Agreement:

DEFINITION

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.

POLICY

Vision for digital technology at MEC

MEC understands that digital technologies 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. They also enable personalised learning tailored to students' particular needs and interests, improved assessment, reporting and feedback and new forms of collaboration and communication. MEC 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. MEC's vision is to empower students to use digital technologies to reach their personal best and fully equip them to contribute positively to society.

Safe and appropriate use of digital technologies

Digital technology, if not used appropriately, may present risks to users' safety or wellbeing. At MEC, 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 MEC, 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 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 students
- have programs in place to educate students to be promoting safe, responsible and discerning use of digital technologies
- educate 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 MEC's *Student Engagement* policy that outlines MEC'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 the earliest opportunity
- educate 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
- support parents and carers to understand safe and responsible use of digital technologies and the strategies that can be implemented at home through regular updates in MEC media platforms.

Distribution of school owned devices to students and personal student use of digital technologies, including BYOSD 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 an appropriate staff member immediately.

All messages created, sent or retrieved on MEC's network are the property of MEC. MEC 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.

Student behavioural expectations

When using digital technologies, students are expected to behave in a way that is consistent with MEC's *Statement of Values, Student Wellbeing and Engagement* policy, and *Bullying Prevention* policy. When a student acts in breach of the behaviour standards of the MEC community (including cyberbullying, using digital technologies to harass, threaten or intimidate, or viewing/posting/sharing of inappropriate or unlawful content), MEC 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 MEC's:
- Digital Technologies Behaviour Management Process (Appendix D)
- *Statement of Values*
- *Student Wellbeing and Engagement* policy
- *Bullying Prevention* policy policies
- *Electronic Communication Device* policy.

REVIEW PERIOD

This policy was last updated on Wednesday 10th December, 2020 and is scheduled for review as part of the school's 3 year review cycle.

This policy was last ratified by School Council on Wednesday 10th December, 2020.

Signed:

Paul Rumpff
School Council President **Date:** 18.12.2020

Appendix A
Bring Your Own Specified Device (BYOSD) Specifications 1 to-1 personal devices

Ownership

- The device is owned by the parents/student but is made available for use as part of the school learning program.
- Parents/students should be aware that files stored on the device are private but may be publicly accessed as part of learning programs. The school reserves the right to inspect a student's personal device if there is reason to believe that the student has violated DET or MEC school policies, administrative procedures, school rules or has engaged in other misconduct while using their personal device.
- Violations of any DET policies, administrative procedures or school rules involving a student's personally owned device may result in quarantine or loss of use of the device in school and disciplinary action.

Software and access

- The school will provide information about standard software programs and applications required for installation on personal devices and will advise when new software or applications need to be purchased.
- Parents are responsible for purchasing and installing new programs on personal devices. Parents are advised to set up a separate family account (not use their own accounts) to manage purchases for their child's device.
- MEC are not responsible for any part of the manufacturer's software, backup, restore, image or individual programs, parents are recommended to use manufacturer's recovery media creation software prior to sending the device to the MEC ICT team for connection/configuration
- The school will provide access to some software and applications through e.g. eduStar www.edustar.vic.edu.au/catalogue/Pages/SoftwareHome.aspx. There is no cost for this access.

School Support

Support will be provided for:

- connecting the device to the school network, internet and other digital technologies
- set up and management of school, student email accounts
- all school-based software and associated issues with school applications.
- a short term loan device for students when their device is begin repaired by LWT (Learning With Technology).

Support will not be provided for:

- connecting to home networks, the internet, printers, or other devices
- personal email accounts and settings
- software issues
- hardware issues on devices not being purchased from LWT

Damage or loss of equipment

- Parents are responsible for making sure the device is covered under their insurance, so that it can be replaced if lost or damaged and student learning is not interrupted.
- The school must be notified if the device is damaged or lost so that a student's learning program is not interrupted whilst being replaced.

Student Responsibilities

Students are responsible for:

- The student is responsible for the proper care of their personal device, including (but not limited to) any costs of repair, replacement or modification needed to use the device at school
- bringing portable devices fully–charged to school every day
- catching up on any work not completed as a result of the student not bringing their laptop to school.
- ensuring the device has appropriate virus protection
- backing up data securely
- carrying their device in an appropriate protective case at all times. The student will keep the device with him/herself at all times or in a secure location. The school does not take any responsibility for the security of the device at all throughout the day.
- adhering to this Acceptable Use Agreement when using the machine, both at home and at school, including during lunchtime or when not in the classroom. The student may not use the device(s) to record, transmit or post photos or video of a person or persons at school or affiliated school programs such as excursions, camps etc. Nor can any images or video recorded at school be transmitted or posted at any time without the written permission of a staff member.
- using their device to access relevant files and websites only.
- using the school and DET secured wireless network. **Use of 3G, 4G and 5G mobile hotspot connections are not permitted at any time.**

<table>
<tr><td colspan="2">BYOSD Requirements:</td></tr>
<tr><td>WIRELESS CONNECTIVITY</td><td>Wireless connectivity is the key to BYOSD device in schools. Device must support 5Ghz dual band wireless which is 802.11 a/b/g/n.</td></tr>
<tr><td>BATTERY LIFE</td><td>Devices need to last the school day; we recommend a minimum of 6 hours battery life.</td></tr>
<tr><td>RAM 8GB</td><td>To be able to store and process data effectively these minimum specifications are recommended.</td></tr>
<tr><td>OTHER ESSENTIALS</td><td>Casing: Needs to be tough and sturdy. Can it be dropped without breaking?
Weight: Is the laptop light enough for the student to carry each day?
Durability: Consider the overall durability of the device; are the keys and inputs sturdy?</td></tr>
<tr><td>SOFTWARE AND APPS
•</td><td>Devices must have software or apps that allow for:
internet browsing
notetaking
word processing
creating spreadsheets
Students have access to a range of licenced software by Microsoft & Adobe for their BYOSD devices through the DET eduSTAR catalogue
creating presentations</td></tr>
<tr><td>SUPPORTED DEVICES</td><td>(Note: Phones, smart phones, personal communication devices eg. music players and watches are not acceptable devices for the BYOSD program).
<table>
<tr><td>PC
Windows 7 or newer</td><td>MAC
OS X 10.9 or newer (MacBook)
iOS 7 or newer (iPad / iPad mini)</td></tr>
</table></td></tr>
<tr><td>ACCESSORIES</td><td>Carry Case: A carry case is essential in protecting your device and can provide ergonomic advantages.
Insurance: Devices can become lost or broken at school, make sure your policy covers these eventualities.</td></tr>
</table>

ANTIVIRUS AND MALWARE	It is essential that each device has up-to-date anti-virus and malware software. Windows and MAC devices must run Microsoft's System Centre Endpoint Protection (SCEP). This can be found and accessed under through the eduSTAR catalogue. iPad's do not have or require Anti-virus software.

Appendix B - Advice for Parents and Students

Please keep this as a resource to use at home

At school, technology and the internet is used to support teaching and learning. However, at home 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, play and chat.

If you have the internet at home, encourage your child to show you what they are doing online.

Loan of Devices

- LWT devices- a student may be able to borrow a short term loan device directly from the MEC ICT department in the case that their device is being repaired.

- Non LWT Devices- families may contact the school to see if a short term loan device is available if the student has a non-LWT device being repaired

At home we recommend you:

- encourage your child to show you what they are doing online
- make some time to sit with your child to find out how they are using the internet and who else is involved in any online activities
- ask them to give you a tour of their 'space' if they are using a site which allows them to chat, publish photos, play games etc.
- always get them to set their space to 'Private' if they use a social networking site (they are then in control of who can contact them and access their information)
- have the computer with internet access set up in a shared place in the house – not your child's bedroom
- negotiate appropriate times for your child's online activities and use of mobile phones
- ask questions when your child shows you what they are doing
    - how does it work, how do you set it up and can you block out people?
    - who else is sharing this space or game - did you know them before or 'meet' them online and what do you know about them?
    - why is this so enjoyable – what makes it fun?
    - can you see any risks or dangers in the activity - what would you say to warn/inform a younger child who was going to start to use the space?
    - what are you doing to protect yourself or your friends from these potential dangers?
    - when would you inform an adult about an incident that has happened online that concerns you?

Please keep this as a resource to use at home

MICROSOFT OFFICE 365 EDUCATION - PRIVACY INFORMATION

Maryborough Education Centre uses *Office 365 for Education* in the classroom as part of our teaching and learning program. Office 365 for Education is an internet based service provided by Microsoft for educational purposes only. It provides students and teachers with access to online services such as email, calendar, blogging, online document storage (for school work), sharing, messaging and video-conferencing facilities from school, and at home. Office 365 for Education include but are not limited to the following online services:

Office 365 Education ('online services')	
1.Exchange online email	6.Yammar
2.Lync online	7.Office video
3.SharePoint online	8.OneNote Classroom
4.OneDrive for Business	9.Microsoft Classroom
5.Microsoft Office apps	10.Sway
Additional Microsoft 'online services' may be added by our school to further support teaching and learning	
Terms and conditions	
Microsoft Online Services Terms and privacy information can be found by clicking on the links opposite:	http://www.microsoft.com/en-us/licensing/product-licensing/products.aspx http://office.microsoft.com/en-us/business/office-365-trust-center-cloud-computing-security-FX103030390.aspx. http://office.microsoft.com/en-us/business/office-365-trust-center-top-10-trust-tenets-cloud-security-and-privacy-FX104029824.aspx.

Microsoft access to specific personal information of your child

To enable your child to sign-on and access these online services as part of our schools teaching and learning program, Microsoft require access to your child's Department of Education & Training username, first and last name, year level and school. You may request that our school not provide this information to Microsoft, and opt-out your child from using Office 365 for Education. As a result, your child will not have access to the online services and alternate arrangements for allocating work will be made.

Parental access to Personal Information

The Department of Education and Training's ('Department') use and handling of your child's personal information is governed by the *Privacy and Data Protection Act 2014 & Health Records Act 2001(Victoria)*. You can access personal information held by the Department about you and your child under the *Freedom of Information Act 1982 (Victoria)*. If a mistake in that personal information is identified, the Department is required to correct it under the *Privacy and Data Protection Act 2014.*
Microsoft's Online Services Terms provides further information on how Microsoft may use your child's personal information.

Providing a safe online environment

Use of online services will be subject to classroom supervision during school hours. Students should report unacceptable behaviour, and a nominated member of staff will address the issue **during school hours.**
To further assist your child in having safe and positive experiences online, you can refer to parent information on the Australian Government's Office of the Children's eSafety Commissioner website.
In addition, staff at our school have been advised that the use of Office 365 for Education is strictly for teaching and learning material only (e.g. lesson plans and classwork) and staff do not upload your child's personal, sensitive, health; or security classified information into Office 365 for Education.

Student responsibilities when using online services

When using Office 365 for Education, students continue to be responsible for their behaviour as outlined in our school's Students Acceptable Use Agreement. The main themes of this agreement are:

- Communicate respectfully;
- Protect personal information; and
- Look after yourself and others.

Purpose of this Privacy Information

The purpose of this Privacy Information and opt-out form is to set out Privacy Information related to Office 365 for Education, and explain:

- you are able to opt-out your child from using the service at any time by written notification to the school.
- how your child's personal information will be collected, used, disclosed and managed.
- that if the school determines that the personal information, or the online services are no longer required or relevant, the use of the personal information and/or the online services will cease.

Should you wish to opt-out your child from using Office 365 for Education, please notify the school in writing. As a result, your child will not have access to the online services and alternate arrangements for allocating work will be made

Appendix C

MEC Digital Technologies Behaviour Management Process

Minor Infringement

Definition: Any activities other than set class work. e.g. Playing games, looking at Memes, reading unrelated sites, checking football scores, personal emails etc.

1st Time – Teacher restates and reteaches the task at hand and which software is to be open.
2nd Time – Student will receive a warning from the teacher.
3rd Time – Student is asked to pack up laptop or close desktop computer. Electronic Personal device will be confiscated as per Electronic Communications Device Policy for remainder of the lesson and the classroom teacher will record Electronic Device Infringement incident on Xuno.
Repetition of Minor Infringements will be followed up in accordance with MEC protocols including parent meetings and network restrictions etc.

Moderate Infringement

Definition:

a. Deliberately bypassing the EduSTAR network via any method, eg: using a VPN or hotspot to access blocked sites but not explicit in nature such as YouTube, Facebook etc. circumventing eduSTAR is an unsafe practice that jeopardises the security of every device.
b. Deliberately damaging a school owned device or BYOSD.
c. Attempting to access other students' accounts.

- Student is asked to pack up BYOSD device for remainder of the lesson. Student is asked to close school laptop, desktop or other device. Electronic Personal Device will be confiscated as per Electronic Communication Device Policy.
- Classroom teacher creates Digital Infringement Helpdesk Ticket.
- IT technician/ICT representative to suspend student from their eduSTAR and network account.
- Classroom teacher records Electronic Device Infringement incident on Xuno.
- Classroom teacher makes phone call or arranges parent meeting before the student account is reactivated.
- Student's internet access may be revoked for an extended period of time.

Major Infringement

Definition: Exposure or suspected exposure to graphic content (including accidental exposure). Accessing graphic content including sexualised content within a school maybe a criminal act.

- Student closes their BYOSD electronic personal device or school owned device immediately and hands it to the teacher. Desktop computer shut down.
- Device is quarantined with an Incident Sticker (located in coordinator, administration assistant in each pod and IT office in Majorca).
- Portable device is locked in coordinator, leading teacher, sub school leader desk until it can be transported to and stored in Principal's Office. Desktop will be removed by IT technician and stored in Principal's Office. The device must not be carried by students.
- Classroom teacher creates Digital Infringement Helpdesk Ticket.
- IT technician/ICT representative to suspend student from their eduSTAR and network account.
- Classroom teacher records Electronic Device Infringement incident on Xuno.
- Coordinator contacts parents and arranges parent meeting before the student account is reactivated and/or device returned.

Student failure to comply with the above process will be managed through relevant MEC policy.

Appendix D – Acceptable Use Agreement

Student declaration

When I use digital technologies and the internet I agree to be a safe, responsible and ethical user at all times by:

- Respecting others and communicating with them in a supportive manner;
- Never participating in online bullying (e.g. forwarding messages and supporting others in harmful, inappropriate or hurtful online behaviours);
- Protecting my privacy by not giving out personal details, including my full name, telephone number, address, passwords and images;
- Protecting the privacy of others by never posting or forwarding their personal details or images without their consent;
- Talking to a teacher or a trusted adult if I personally feel uncomfortable or unsafe online, or if I see others participating in unsafe, inappropriate or hurtful online behaviour;
- Thinking carefully about the content I upload or post online, knowing that this is a personal reflection of who I am and can influence what people think of me;
- Reviewing the terms and conditions of use for any digital or online tool (e.g. age restrictions, parental consent requirements), and if my understanding is unclear seeking further explanation from a trusted adult;
- Meeting the stated terms and conditions for any digital or online tool, and completing the required registration processes;
- Handling ICT devices with care and notifying a teacher of any damage or attention required;
- Abiding by copyright and intellectual property regulations by requesting permission to use images, text, audio and video, and attributing references appropriately;
- Not accessing media that falls outside the School's policies;
- Not downloading unauthorised programs, including games;
- Not interfering with network systems and security or the data of another user;
- Nor attempting to log into the network with a user name or password of another student.
- Bringing my device to school everyday fully charged.
- Understanding that there actions and consequences established within school policies if I do not behave appropriately.

In addition, when I use my personal mobile phone I agree to be a safe, responsible and ethical user at all times, by following the MEC ECD policy and:

- Keeping my device silent, invisible and unseen between 9am and 3:15pm;
- Only taking and sharing photographs or sound or video recordings when others are aware the recording is taking place and have provided their formal consent as part of an approved lesson.

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.

Please select one option below:

□ I understand and agree to:

- comply with the terms of acceptable use and expected standards of behaviour set out within this agreement and the MEC ECD policy
- receiving access details to use digital technologies (digital devices, tools, applications and systems that students use for learning).
- abide by the **Bring Your Own Specified Device** guidelines. I further understand that any violation of the guidelines may result in the loss of network and/or device privileges as well as other disciplinary action.

□ I would like to discuss further with someone before I sign this agreement

Student name: _____

Student signature: _____

Parent/Guardian Name: _____

Parent/Guardian Signature: _____

Date: _____