THE MARIST SCHOOL ASCOT

School DfE No: 868/6013

DIGITAL POLICY

Policy Number: DP008

Excellence as a habit not an action.

Excellence in who we are; Excellence in what we do; Excellence in our service of others.

Digital Policy

Revision	Date	Amendment	Completed By:	Authorised By:
1	21/01/2025	Creation of Policy	CB	SA

DIGITAL POLICY

CONTENTS

PURPOSE OF THE POLICY:

This policy gathers the following policies into one document:

- Acceptable Use Policy
- Student Device Policy including Bring Your Own Device (BYOD)
- Artificial Intelligence Policy
- Cyber Attack Policy

The aim of this policy is to:

- Provide clear guidelines for student use of both school-issued devices and BYOD.
- Outline acceptable use of devices connected to the school network.
- Protect the school network and equipment from damage or misuse.
- Ensure students use technology in a safe, responsible, and secure way.
- Comply with relevant regulations.

DIGITAL POLICY SUMMARY

Parent/Student Agreement - Parents and students must agree to the content of this Policy by completing the relevant section at the end of this policy to show acceptance of the terms and conditions of the use of digital devices in school before they are permitted to use them.

Security and Care - Students are responsible for the proper care and use of their device. Students are responsible for charging their device overnight. They are also responsible for the adequate security of their device whilst in school, keeping it with them when required or securing properly in their own locker. It is recommended that students do not share or lend their devices or peripherals (e.g. stylus) to other students.

Educational use – Devices will only be used for educational purposes to support learning whilst in school and at home. It will be at the teacher's discretion as to when these devices may be used by a student within the lesson. Students will respect a teacher's decision and turn off their device when requested to do so.

Audio, Photographs and Video – Students will not directly or indirectly via another student use their devices to record audio or take photographs or videos of other students or members of staff without permission for educational purpose. Students will not store or share media of others without permission from a member of staff.

Internet Usage Policy – All devices must access the internet through The Marist School's network filtering system. Students will adhere to the school's Acceptable Use Policy. In addition, students will not access any inappropriate material that may or may not already be downloaded onto their device.

Students breaching this Policy – If a student breaches this Policy or if a member of staff feels that they are likely to have breached this policy then the student's device may be confiscated pending investigation, and the student's parents may be contacted. Subsequent breaches of this policy with be dealt with by a member of the leadership team.

DIGITAL DEVICE POLICY:

DEVICES COVERED UNDER THE POLICY:

SCHOOL ISSUED DEVICES – LAPTOPS ISSUED **BEFORE** SEPTEMBER 2024:

These are devices that were issued prior to September 2024 and are managed and owned by the school.

OVERVIEW

Although the device is owned by the school, students should treat it as their own device and take reasonable care of it. Repair of any damage to the school issued laptop will be arranged through the school and you will be billed for the expense of the repair, plus an admin fee of £50. From September 2024 if the device is lost or damaged beyond reasonable repair, parents will be migrated to the new laptop scheme offered through Easy4U. Details can be found in the School Managed Devices' section below. If the laptop accessories are lost or damaged, they will need to be replaced through the school, and you will be billed for this expense. School owned laptops and accessories must be returned to the school upon graduating or withdrawing from the school or you will be charged.

SCHOOL MANAGED DEVICES – LAPTOPS ISSUED **AFTER** SEPTEMBER 2024:

These are devices that are managed by the school but are owned by the parents.

OVERVIEW

The Easy4U rental program offers laptops on an outright purchase or lease program from 24 to 60-month terms, covering the device, software installation, service, support, and insurance. On the rental scheme a four-month deposit is required upfront, but there are no credit checks, and you can return the device at any time. After the rental period ends, you can either return the device for a deposit refund (assuming responsibility for software licensing) or keep it. The school receives no commission for this partnership. The device will be managed by the school and come with all required software installed. **Full details of the scheme can be found in the Easy4U documentation provided to all parents**.

BRING YOUR OWN DEVICES (BYOD)

From time-to-time students may have reason to bring their own devices to school, in addition to their school devices, for educational purposes. This may include, but is not limited to laptops, iPads, tablets, and smartphones.

Personal devices are brought into the school at your own risk. By signing the agreement at the end of this policy you acknowledge that you are responsible for all costs associated with your device and that you understand that your usage of your device will be monitored.

All personal devices brought into the school will need to connect to the internet through the schools Wi-Fi, which may involve the installation of software. Any device connected to the school network will need to follow the policy details outlined below.

To minimise distractions, students are required to hand in their mobile phones to their form tutor upon arrival, which will be securely stored for the day.

DIGITAL POLICY DETAILS

1. **About this policy**
   - **1.1.** The purpose of this policy is to establish a clear and consistent framework for the use of digital devices within the school.
   - **1.2.** This policy sets out the circumstances in which we may monitor students use of school systems, access your device and retrieve, remove or destroy data on it and the action which we will take in respect of breaches to this policy.
   - **1.3.** The policy is designed to protect school systems while enabling the student to access our systems using a device.
   - **1.4.** Anyone covered by this policy may use a digital device for learning purposes, provided that they sign the agreement at the end of this policy and adhere to its terms.
   - **1.5.** This policy covers all students on roll at The Marist School.

2. **Personal responsibility for this policy**
   - **2.1.** The Executive Leadership Team has overall responsibility for the effective operation of this policy but has delegated the day-to-day responsibility for its operation to the Deputy Head. The Deputy Head is responsible for reviewing this policy to ensure that it meets legal requirements and reflects best practice.
   - **2.2.** The Deputy Head has responsibility for ensuring that any person who may be involved with the administration, monitoring, IT security or investigations carried out under this policy receives regular and appropriate training to assist them with these duties.
   - **2.3.** All staff and students at The Marist School are responsible for the success of this policy.
   - **2.4.** Any misuse (or suspected misuse) of a device or breach of this policy should be reported to the Deputy Head.
   - **2.5.** If you have any questions regarding this policy or have questions about the use of digital devices for learning purposes which are not addressed in this policy, please contact the school.

3. **Scope and purpose of the policy**
   - **3.1.** This policy applies to students who use a school issued device, school managed device or BYOD, including any accompanying software or hardware for learning purposes.
     - **3.1.1.** For school owned or managed devices this applies to use of the device both during and outside school hours.
   - **3.2.** This policy applies to all devices used to access our IT resources and communications systems (collectively referred to as systems in this policy).
   - **3.3.** When the school system is accessed using a device, it is exposed to a number of risks, including the threat of malware (such as viruses, worms, spyware, Trojans or other threats that could be introduced into our systems via a device). This could result in damage to school systems. The school will manage school issued and school managed devices to ensure the device is kept up to date to minimise the risk of these threats on the device.
   - **3.4.** Breach of this policy may lead to the school revoking access to school systems, whether through a device or otherwise. It may also result in sanctions up to and including exclusion. Students are required to co-operate with any investigation into a suspected breach, which may involve providing us with access to the device and any relevant passwords and login details.
   - **3.5.** Some BYODs may not have the capability to connect to the school systems. The school is not under any obligation to modify its systems or otherwise assist students in connecting to those systems.

4. **Connecting devices to school systems**
   - **4.1.** Connectivity of all devices is centrally managed by The Marist School IT Support team.
   - **4.2.** In order to access school systems, it is necessary for The Marist School IT Support team to install software applications on the device. If you remove or attempt to remove any such software, access to our systems will be revoked.
   - **4.3.** The school reserves the right to refuse or remove permission for a device to connect with the school systems. The Marist School IT Support will refuse or revoke such permission (and may take all steps necessary to do so) where in our reasonable opinion a device is being or could be used in a way that puts, or could put, the school, our students, our staff, our systems, or sensitive data at risk or that may otherwise breach this policy.

5. **Monitoring**
   - **5.1.** The school reserves the right to monitor, intercept, review and block, without further notice, any content on the device.
   - **5.2.** Monitoring, intercepting, reviewing or blocking is carried out in order to:
     a) prevent misuse of the device.
     b) ensure compliance with our rules, standards of conduct and policies in force.
     c) prevent harm to the school's IT systems.

6. **Security requirements**
   - **6.1.** Students must comply with our Acceptable Use Policy when using devices.
   - **6.2.** The school reserves the right, without further notice or permission, to inspect the device, access data and applications on it, and remotely review, copy, disclose or wipe, enabling us to:
     a) inspect the device for use of unauthorised applications or software, such as VPN software.
     b) investigate or resolve any security incident or unauthorised use of school systems.
     c) ensure compliance with our rules, standards of conduct and policies in force.
   - **6.3.** If the school discovers or reasonably suspects that there has been a breach of this policy including any of the security requirements listed above, your access to school systems will be immediately removed.

7. **Damaged, Lost or Stolen devices**
   - **7.1.** Lost or stolen devices should be reported to the students Head of Year immediately.
     - **7.1.1.** For School owned or managed devices this will start a search process to try and locate the device.
     - **7.1.2.** If the device is not located, we will then attempt to wipe the device remotely, therefore students should ensure all documents are always saved on their OneDrive only.
     - **7.1.3.** Devices that have not been located but were purchased through the Easy4U Digital Device Scheme are fully covered and you will have the option to inform the insurance company yourself or to request the school to manage this process. The excess on each claim is payable by the parent to the insurance company.
     - **7.1.4.** If a school managed device is damaged beyond reasonable repair, determined by the school, parents will be migrated onto the Easy4U scheme.
   - **7.2.** The school takes no responsibility for damaged, lost or stolen devices.

8. **Technical Support**
   - **8.1.** We provide technical support during school hours for school issued or managed devices. Students need to bring their device to school for support to be provided.
   - **8.2.** Students are responsible for reporting any issues as soon as possible. The school will deal with any software installations and updates, but repairs and replacement costs will be chargeable to the parent, or in the case of school managed devices acquired through the Easy4U scheme parents will be responsible for making a claim.
   - **8.3.** We do not provide technical support for BYOD's. If a BYOD is brought in to school you are responsible for any repairs, maintenance or replacement costs.

GENERAL RULES FOR DEVICE USAGE:

LAPTOP USAGE:

- ✓ Laptops should be fully charged overnight.
- ✓ Laptops should only be used for educational purposes.
- ✓ Laptops should remain closed until asked to open them by a teacher.
- ✓ Emails should be checked daily, and emails deleted once they have been dealt with.
- ✓ Important dates should be recorded in the Outlook Calendar and should be checked frequently.
- ✓ At lunchtime you are expected to be off the devices and engaging with other students or co-curricular activities.

SECURITY OF LAPTOPS:

- ✓ Keep your log in details private and only use your own device.
- ✓ Ensure you lock your device if you leave it unattended to ensure no one else can access your account.
- ✓ Laptops should be kept securely at all times, including travelling to and from school.
- ✓ No additional software (apps) should be installed without permission.

ACCEPTABLE USE POLICY (AUP)

SECTION OVERVIEW

The following section of the policy sets out the requirements for students when using IT facilities. All students are expected to adhere to this policy.

BEHAVING RESPONSIBLY ONLINE

The following principles should be adhered to when using devices whether on school property or at home:

- All communication with students, teachers and others is polite and respectful.
- Understand that online activity, both in and outside of school, is as important as conduct in person. Students will not engage in any online behaviour that could cause the school, its staff, students or others distress or bring the reputation of The Marist School into disrepute.
- Students will not deliberately browse internet sites, or view content that is illegal, violent or considered offensive (for example material that is racist, sexist or that promotes violence, terrorism, religious extremism or discrimination) and recognise that the school is able to monitor online activity and that any attempt to view inappropriate content online could result in a disciplinary procedure being followed.
- Students must not search online for, or view, publications that undermine the fundamental British values of democracy, the rule of law, individual liberty, and mutual respect for and tolerance of those with different faiths and beliefs and for those without faith.
- Students will follow, and respect, copyright law and plagiarism legislation when operating safely online.
- If the AUP rules are not followed, school sanctions will be applied in line with the school Behaviour Policy, and that online privileges within The Marist School's network may be temporarily, or permanently, removed.

USE OF THE SCHOOL'S IT FACILITIES

The following guidelines must be followed when using school IT systems:

- Students will respect and look after the school's IT equipment. Whilst in the IT suites, students must not eat or drink and that if they are found doing so appropriate disciplinary procedures will be followed.
- Students agree to only log on to the school systems, with their username and password. They will not share their school username and password with anyone else and understand that they should never ask another user for their logon details.
- Students must not attempt to download or install software onto school equipment.
- Students must not attempt to bypass the school's internet filtering system.
- Students must not attempt to circumvent the school's IT security controls, access or delete school data or damage school IT equipment or systems.

OPERATING SAFELY ONLINE

The following guidelines aim to encourage safe online practices and hope to avoid negative consequences arising from the misuse of digital technologies.

- If students encounter difficulties because of online bullying or negative behaviour, then they are encouraged to talk to a teacher, or other trusted member of school staff. This also applies if they are worried about something they may have done online having a negative impact upon others.
- Students must not give out any personal information online that might identify themselves. Such as: home address, telephone number, passwords, or any other sensitive information. Students will also respect the privacy of others and will never compromise their safety and security by making public their personal information.
- Students will not retaliate or reply to offensive emails or messages but instead should report the incident to parents or a trusted member of school staff.

- Students should understand that online contacts may lie about their identity, that information on the internet can be unreliable and that they should be cautious about who and what they believe. If students believe that they, or another member of the school community, may be at risk because of online 'friendships', they must discuss this with a responsible adult that they know and trust.
- Students should be aware that those who seek to promote terrorism or religious extremism may attempt to contact or recruit young people via the internet, and they should never go in search of, or respond to, any communication of this nature.
- Students will ensure that their privacy settings are set correctly when using social media and understand that, just as in the real world, things they do and say online have consequences which will at times need to be dealt with under the school's Behaviour Policy. They should consider their 'digital reputation' before making posts online.

USE OF ARTIFICIAL INTELLIGENCE (AI)

PURPOSE OF THIS SECTION OF THE POLICY

This section outlines the guidelines and expectations for the appropriate and ethical use of Artificial Intelligence (AI) technologies at The Marist School. It applies to all students, staff, and members of the school community.

WHAT IS AI

Artificial intelligence (AI) is a rapidly developing technology that has the potential to revolutionise education. AI can be used to personalise learning experiences, provide feedback, and automate tasks, all of which can help students learn more effectively. AI can help to increase access to education by providing students with the opportunity to learn from anywhere, at any time. We recognise in particular that Generative AI, and its use in education, is still in its early stages of development and will continue to evolve over the coming months and years. As best practices for the use of AI emerge, we will continue to develop and adapt our policies accordingly.

At the Marist we recognise the importance of integrating Artificial Intelligence (AI) technology into our educational practices while upholding our core values as a Catholic school. This AI policy aims to provide a framework for the responsible and ethical use of AI within our school, ensuring the well-being and educational development of our students.

RESPONSIBLE USE OF AI

Educational Purposes: Students are encouraged to use AI technologies for educational purposes, such as research, learning, and creative projects, under the guidance of their teachers, when appropriate.

Ethical Considerations: Students should use AI in a manner that upholds the school's values, promotes fairness, inclusivity, and respect for others. AI usage should not discriminate, harm, or invade privacy.

Personal Data: Students should be mindful of the privacy and confidentiality of personal data when using AI technologies. They should not share personal information of themselves or others without consent as when you interact with AI, your inputs are used to train and improve its understanding.

Original Work: Students should use AI technologies to support their learning and creativity while maintaining academic integrity. Plagiarism or dishonest use of AI-generated content is strictly prohibited.

Attribution: When using AI-generated content or incorporating AI tools in their work, students should properly reference the source.

Bias and Discrimination: Students should be aware of the potential biases in AI systems and take steps to critically evaluate and address any discriminatory outcomes.

REPORTING STUDENT CONCERNS

Reporting Misuse: Students are encouraged to report any misuse or concerns related to the use of AI technologies to a trusted member of school staff.

Support and Guidance: Students can seek assistance and guidance from school staff regarding the responsible use of AI technologies.

Usage in NEAs and Coursework:

There are strict guidelines issued by the JCQ (Joint Council for Qualifications) on the acceptable use of AI when completing NEAs, coursework and other internal assessments. Teachers have received training covering this content.

At the start of the academic year students will receive training on how to use AI ethically using permitted AI tools during coursework, in line with JCQ's regulations. This training will equip them to distinguish between approved resources, like grammar checkers, and prohibited ones. It will also clarify expectations for citing AI-generated content and reinforce the importance of showcasing their own original work. Please see the **appendix 1** for an overview of the acceptable use of AI in coursework in and NEA's.

CYBER ATTACK POLICY

PURPOSE OF THIS SECTION OF THE POLICY

Our school takes online safety and security very seriously. This policy outlines how we will work together to protect our school network, student data, and personal information from cyber-attacks.

WHAT IS A CYBER ATTACK?

A cyber-attack is any attempt to damage, disrupt, or steal information from a computer system or network. This can include things like:

Malware: Malicious software like viruses, worms, and ransomware that can infect devices and cause damage.

Phishing: Emails or messages that try to trick you into revealing personal information or clicking on malicious links.

Hacking: Unauthorised attempts to access a computer system or network.

OUR RESPONSIBILITIES

THE SCHOOL WILL:

- Implement security measures to protect network and data.
- Have a plan to respond to cyber-attacks in a timely and effective manner.
- Report any suspected cyber-attacks to the appropriate authorities.

STUDENTS MUST:

- Use school devices and accounts responsibly and in accordance with the school's Acceptable Use Policy.
- Be aware of the risks of cyber-attacks and how to protect themselves online.
- Report any suspicious activity, such as phishing emails or malware, to the IT department immediately.
- Use strong passwords and keep them confidential.
- Avoid downloading unauthorised software or visiting unsafe websites.

APPENDIX 1: AI AND ASSESSMENTS A QUICK GUIDE FOR STUDENTS

JCQ Guidelines Poster for Students on Acceptable use of AI in assessments

Ratified: 23rd September 2024 **Renewal: December 2027 (oar)**

Signed:

Mrs Jo Smith

Principal