Student Technology Acceptable Use Policy

A QUICK REFERENCE GUIDE

Students at Marymount are encouraged to use and enjoy the latest technology to support and enhance the learning experience as long as it is used in a safe and appropriate manner. We ask that students adopt good working habits and try to regulate how much time they spend on their devices. Students should remember to turn off their computers in order to engage with others and participate fully in a range of activities. They are responsible for exercising good judgment and behaviour whilst using the School's IT equipment. Any use of Technology that brings the School into disrepute will be treated with the utmost seriousness and will result in disciplinary action.

The following is designed to provide you with a basic guide to the safe and acceptable use of all technology at Marymount International School London (including but not limited to Computers, Tablets, Mobile Phones and MP3 players).

BASIC SAFETY:

- The School uses a web filter to help ensure content from the Internet is appropriate when accessed from school premises. Parents should activate the appropriate Parental Controls on all their daughter's devices to support safety and security.
- You may only log on to the school network as yourself. Do not use someone else's logon name or password or share your login and password details to anyone else or allow anyone else to use them.
- Be aware that the School can check your network logs at any time to see which sites you visit and messages sent on school systems.
- Do not use bad language, bully or try to access inappropriate material online.
- Mobile Phones and MP3 players must be switched off and out of sight during lessons unless permission has been given by the teacher to use them.
- Middle School students may bring mobile phones to School but they must remain switched off during the School day and may only be used with the express permission of the Middle School Coordinator.
- During the school day, High School students may use mobile telephones only at break, lunch and/or study periods and only in the designated areas.
- Computers, tablets and internet browsers may not be used during lessons unless permission has been given by the teacher to do so.
- Under no circumstances are you to use social networking sites, personal email or video call (Skype, Facetime etc.) during the school day.
- You are not to record anything during lessons unless the teacher requests that you do so.
- You must not wear earphones when walking around the campus at any time.
- Attempting to bypass the School's web filters by using 3G/4G/5G-capable devices and/or VPNs (Virtual Private Networks) to access the internet is strictly prohibited.

- Do not give out your personal details online and never arrange to meet a stranger.
- Respect copyright and do not plagiarise work.
- During the school day, you may only use computers for educational purposes.
- The taking, possession or distribution of indecent images is strictly forbidden.

Any breach of this policy will result in appropriate disciplinary action.

INTRODUCTION

The use of the latest technology is actively encouraged at Marymount International School but with this comes a responsibility to protect students, staff and the School from abuse of the systems. All students, therefore, must adhere to the Policy set out below. This Policy covers all workstations, laptops, tablets, mobile telephones and all other electronic devices within the school, irrespective of who is the owner.

All students are expected to behave responsibly on the school computer network, as they would in classrooms and in other areas of the school.

(Related Policy and Guidance can be found in the Online Teaching and Learning Policy)

ONLINE SAFETY

SMART RULES

S **Safe:** Keep safe by being careful not to give out any personal information, such as your full name, email address, telephone number, home address, photos or School name, to people you have only had contact with online.

M **Meeting:** Meeting someone you have only been in touch with online can be very dangerous. Only do so with your parents' or guardians' permission and even then only when they can be present.

A **Accepting:** Accepting emails, instant messages, or opening files, pictures or texts from people you don't know or trust can lead to problems; they may contain viruses or nasty messages!

R **Reliable:** Information you find on the Internet may not be true, or someone online maybe lying about who they are.

T **Tell:** Tell your parents, guardian or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.

Students or parents can report online abuse to the police at: www.thinkuknow.co.uk and you can report anything you are not happy about to anyone you feel you trust. This could be your Advisor, a teacher, Houseparent, your guardian, parent or someone else's parent. Tell someone!
For Social Media and to consider the levels of respect and kindness that build our School community, before you post consider:

T Is it **TRUE**?
H Is it **HELPFUL**?
I Is it **INSPIRATIONAL**?
N Is it **NECESSARY**?
K Is it **KIND**?

It is important that all students at Marymount are aware of the risks involved when using the internet. The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

- content: being exposed to illegal, inappropriate or harmful content.
- contact: being subjected to harmful online interaction with other users.

- conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and
- commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel you are at risk, please report scams to the Anti-Phishing Working Group (https://apwg.org/).

Should any student feel they are at risk online, they should immediately speak to the Designated Safeguarding Lead, member of faculty or parent/guardian.
To address the issues named above, students will be taught how to avoid the associated risks through their PSHEE curriculum, the Advisory curriculum as well as assemblies and workshops / presentations.

TO HELP PROTECT YOURSELF FROM THE ISSUES NAMED ABOVE:

- Always be extremely cautious about revealing personal details and never reveal a home address, telephone number, school name, picture /image/live stream/video or email address to strangers, especially people you have only encountered online.
- Always be yourself and do not pretend to be anyone or anything that you are not on the Internet.
- Do not arrange to meet anyone you have only encountered online; people are not always who they say they are.
- Do not send anyone your credit card details or anyone else's or any other details without checking with an adult first.
- Always inform your teacher or another adult you trust if you have visited a website or received a message that contains inappropriate language or that makes you feel uncomfortable in any way or if you think someone is being bullied.
- Remember that Chat / Dating / Live-streaming activities online can put you in danger and for this reason should be avoided or used with extreme caution and with the highest security settings available. Letting a trusted adult know that you are engaging in online live streaming or chat is advised.
- Do not engage in social media or messaging services during the school day. Ensure that privacy settings are set to friends only (avoid default public settings). Social media or messaging services should only be accessed with parental permission and should be age appropriate (see age settings for each app: https://www.internetmatters.org/) Do not provide links to private information or images in your public social media profiles (e.g photo editing or storage software).
- If someone makes you an offer on the web or via email which seems too good to be true, it probably is.
- Extremism and Radicalisation: Some extremist groups who advocate violence use the internet as a means of radicalisation, inciting violence and promoting methods of terrorism. Accessing websites containing such material would be a breach of this policy. These groups pose a threat both to individuals and to society in general and it is everyone's responsibility to report concerns. If you come into contact with any such material or communication online or are aware that anyone else is accessing such material you must report it, as you would any Safeguarding concern, to the School's Designated Safeguarding Lead. If you have accessed material in error or have been contacted by any such group reporting this immediately enables the School to act in protection of you and the community.
- If in doubt, speak to a teacher or another member of staff.

SYSTEM SECURITY

- Do not attempt to go beyond your authorised access. This includes attempting to log on as another person, sending e-mails whilst masquerading as another person or accessing another person's files. Attempting to log on as staff or as a member of the school's IT team is unacceptable and may result in the loss of access to systems and other serious sanctions up to and including exclusion. You are only permitted to log on as yourself.
- Do not attempt to bypass the school's web filters. This includes through the use of 3G/4G/5G capable devices and VPNs. Such attempts are unacceptable and may result in the loss of access to systems and other sanctions up to and including exclusion. Parents are advised that if students have 3G/4G/5G enabled devices they can bypass our security and filters, and therefore we ask that they set up parental controls via their network provider. Each individual network provider can give advice on the controls available via their systems.
- Do not give out your password to any other student; if you do and they do something wrong logged on as you, you will be held responsible. If you suspect someone else knows your password, change it immediately.
- Students should not use the password for Microsoft 365 for any other login, school or otherwise.
- Students must use strong passwords. The UK National Cyber Security Centre recommends three random words. Marymount expects students to use this advice, adding special characters and numbers to strengthen the password. The password should be at least 12 characters long.
- Do not make deliberate attempts to disrupt the computer system or destroy data, e.g. by knowingly spreading a computer virus.
- Do not alter school hardware in any way.
- If you wish to access files on removable media (such as CDs, flash drives etc.) or use mobile equipment (e.g. laptops, tablet PCs, PDAs etc.), please see the IT Office to ensure this equipment has been found clean of viruses, before connecting them to the school system.
- Do not knowingly break or misuse headphones or any other external devices, e.g. printer, mouse, speakers etc.
- Do not attempt to connect to another student's laptop or device at School. Establishment of your own computer network is not allowed.
- Do not tamper with or remove any cables that are attached to a school computer.
- Do not eat or drink whilst using the computer equipment.
- Do not play physical games by or near any computer equipment.

INAPPROPRIATE BEHAVIOUR WHEN USING TECHNOLOGY

'Inappropriate Behaviour' relates to any electronic communication, whether email, blogging, tweeting, social networking, live streaming, texting, sexting, journal entries or any other type of posting/ uploading to the Internet.

- Microsoft Teams and school software must only be used for school purposes. The use of the 'Chat' or 'Meet' functions or messaging must only be for educational or pastoral purposes and not for personal or social reasons. As such, language must always be respectful and appropriate.
- Do not take, post or share a photo or recording of another student or member of staff without their permission.
- Do not contact any member of staff on social media or send friend requests until 5 years following graduation from Marymount or the school from which you graduate from. Linkedin may be used to contact staff after 3 years following graduation for professional networking reasons only.

- Do not take, keep or distribute offensive or indecent images.
- Do not use indecent, obscene, offensive or threatening language.
- Do not post or send information that could cause damage or disruption.
- Do not engage in personal, prejudicial or discriminatory attacks.
- Whilst on campus, students are only permitted to watch age-appropriate content from streaming services or on televisions.
- Do not harass another person. 'Harassment' is persistently acting in a manner that distresses or annoys another person.
- Do not knowingly or recklessly send or post false, defamatory or malicious information about a person.
- Do not post or send private information about another person without their prior agreement.
- Do not use the Internet for gambling.
- Bullying and Cyberbullying of another person either by email, online or via texts will be treated with the highest severity. (See Anti-Bullying Policy and Behaviour, Rewards and Sanctions Policy).
- Do not access material that is profane or obscene, or that encourages illegal acts, violence or discrimination towards other people. NB - If you mistakenly access such material, please inform your teacher or another member of staff immediately or you may be held responsible.
- If you are planning any activity which might risk breaking the Acceptable Use Policy (e.g. research into terrorism for a legitimate project), an appropriate member of staff must be informed beforehand.
- Do not attempt to use proxy sites on the Internet. The School has put filters in place to limit access to sites that would bring the School into disrepute or mean the safety of students is jeopardised. If a student was to access such sites through their own means, they would face disciplinary action.

EMAIL

- Be polite and appreciate that other users might have different views to your own. The use of strong language, swearing or aggressive or bullying behaviour is unacceptable.
- All students will be provided with a Marymount email account. This account should be used to communicate with Marymount teachers and staff. Under no circumstances should you use your personal email account / social media account or messaging service (Gmail, Hotmail, Yahoo!, Instagram, Whatsapp etc.) to contact Marymount teachers and/or staff.
- You should check your School email at least once a day during term time for new messages.
- Do not reply to spam emails as this will result in more spam. Inform the IT Office.
- Do not open an attachment from an unknown source. Inform the IT Office as it might contain a virus.
- Do not open any email that looks suspicious. Inform the IT Office before opening it.
- All emails sent from the School reflect on the School name so please maintain the highest standards.
- Do not send or forward annoying or unnecessary messages to a large number of people, e.g. spam or chainmail.
- Do not join mailing lists without the prior permission of the IT Office.
- Only send mail to a distribution list if you really have to.
- If you receive an email sent to you in error, please inform the sender as soon as possible.
- If you receive an email containing material of a violent, dangerous, racist, discriminatory, defamatory, offensive, in breach of copyright or other inappropriate content, always report such

messages to a member of staff. The sending or receiving of an email containing content likely to be unsuitable for children or schools is strictly forbidden.

PLAGIARISM AND COPYRIGHT

- Plagiarism is taking the ideas or writings of others, including through the use of AI and presenting them as your own. Do not plagiarise works that you find on the Internet or anywhere else. (See Policy on Academic Honesty).
- You cannot assume that information available on the Internet is in the public domain. Information may be protected by copyright or other laws. Although you can read the information, you should not incorporate it into your own work or make a copy to distribute to others without first ensuring you have the legal right to do so. This includes music files and the copying of CDs, downloading of film or music from illegal sites and other such formats. Information obtained from untrusted sources, such as personal web pages or Internet discussion groups may also be unreliable and misleading.

PRIVACY

- All files and emails on the system are the property of the School. Computer storage areas and removable disks will be treated like school lockers. As such, system administrators and staff have the right to access and review them, to ensure that you are using the system responsibly.
- Do not assume that any email sent on the Internet is secure.
- The School reserves the right to randomly search the Internet for inappropriate material posted by students and to act upon it.
- All network access, web browsing and mails on the School system are logged for at least 30 days and monitored to ensure appropriate use and that the School policy is being adhered to. Should inappropriate use of the network, email or internet be apparent, disciplinary action up to and including exclusion, and where necessary, referral to the authorities / police will take place.
- If you are suspected of breaking this Policy, your own personal laptop/device and mobile telephone can be searched by staff.
- If there is suspicion that a student may have banned content such as indecent/pornographic images held on their devices, the Headteacher or a member of staff authorized by the Headteacher may confiscate and search the device without consent from the student or parents but in the presence of another member of staff who is the same sex as the person who owns the device. Should there be reasonable grounds to suspect an image constitutes an offence, the device will be given to the police at the earliest opportunity.
- The school provides all students with access to Microsoft 365, for storage, collaboration, and learning. To ensure data security, maintain student privacy, and comply with school guidelines, students are required to use Microsoft 365 for all school-related activities, including but not limited to creating, storing, sharing, and collaborating on documents, presentations, and projects. Use of other cloud storage and collaboration platforms such as Google Drive, Dropbox, or similar services for school-related activities is not permitted unless explicitly authorized by a teacher or IT department.

SOFTWARE

- Do not install or attempt to install or store software including virus scanners on the School system.
- Do not attempt to download programs from the Internet on to School computers.

- Do not knowingly install spyware, key loggers or any sort of hacking software or device.

SANCTIONS

- Sanctions will vary depending on the severity of the offence; they will range from a warning or withdrawal of Internet use to suspension or expulsion.
- A breach of the law may lead to the involvement of the police.

GENERAL AND BEST PRACTICE

- Boarding: Grades 6-8 students must submit all mobile technologies to houseparents at bedtime. High school students may also choose to do so if they feel it will help with their wellbeing and sleeping patterns. If staff feel devices are being misused or impacting a student's wellbeing, then staff can insist that the device is handed in.
- Think before you print: printing is expensive and consumes resources, which is bad for the environment. Do not waste paper and ink by printing unnecessarily and do not forget to collect your printed materials from the printer.
- Do not send emails to the entire school mailing list. If you feel you need to inform all students or staff, speak to your Advisor and they will send the email on your behalf if deemed appropriate.
- Downloading music, using file-sharing websites, peer to peer applications, scanning or printing photographs for personal use is not permitted on the School network without the express permission of a teacher or other member of staff.
- Always lock or log off your computer when you have finished using it. Do not lock a shared computer so that others cannot use it.
- Always back up your work if you are not saving it on the School system. We recommend creating and saving all school files into your OneDrive, this will ensure they are sufficiently backed up and allow you to use the auto-save function when working in the Microsoft Office suite.
- Observe Health and Safety guidelines; look away from the screen every 10 minutes to rest your eyes and make sure your chair is positioned and adjusted to the correct height for the desk.
- Housekeep your email regularly by deleting old mail.
- If a web page is blocked that you feel you have a legitimate use for, please ask a member of the IT team and it can instantly be unblocked if approval is given.
- The Internet can become addictive. If you feel you are spending too long on it, please ask a teacher or another member of staff for advice.
- If in doubt, ask a member of the IT team.

OTHER ELECTRONIC DEVICES

- The IT Policy above also covers other electronic devices such as laptops, mobile telephones, game consoles and any web enabled device while they are being used at School. However, none of these devices are covered by the School's insurance and the School accepts no liability for them.
- All devices should be security marked and kept locked away where possible. This also includes items such as digital cameras and personal DVD players, etc.

MOBILE PHONES

- Do not use a mobile telephone during lessons unless you have the teacher's permission. Middle School students must submit their mobile phone to the School Office as they arrive to school and collect it at the end of the day. Should a student wish to contact home, they may use a phone in

the School Office. High School students may use their mobile phones during break, lunch and unscheduled times.

- Do not take photos or videos with any device during lessons unless the member of staff has given permission.
- Do not take photos / videos of people without their permission.
- Bullying or harassment (including child-on-child abuse) by text or any other method will be treated seriously as any other form of bullying or harassment, and any student who is found to have bullied or harassed another member of the school community will be subject to the appropriate sanction. (Please see the Safeguarding Policy, Anti-Bullying Policy and the Behaviour, Rewards and Sanctions Policy).
- Do not attempt to hack into someone else's device via Bluetooth or any other method.

MUSIC/VIDEO PLAYERS (E.G. IPODS/AIRPODS /EARPODS)

- The use of such devices is banned during lessons unless the teacher has given permission.
- Do not connect such a device to the School network/School computers.
- Do not break copyright laws by swapping illegal music/video files.
- Do not listen to music in lessons unless the teacher has given permission.

Amended: **July 2023**
To be reviewed: **November 2023**

Student IT Acceptable Use Policy Form

STUDENT:

I have read and I understand the School's Student IT Acceptable Use Policy. I shall use the computer system, internet, school network and school or personal devices in a responsible way and accept the conditions as outlined in the Policy.

Signed:

Printed Name: Date:

PARENT/GUARDIAN

As a Parent or Guardian I have read this agreement. I understand that although Marymount International School employs mail and web defence technology, no system can be 100% safe. I have activated appropriate Parental Control on all my daughter's devices. I give my daughter permission to use the School's network and computer system:

Signed:

Printed Name: Date: