



**Marymount**  
INTERNATIONAL SCHOOL LONDON

## **Marymount Online Safety Policy**

### **Policy Overview:**

The purpose of this policy is to safeguard and protect all members of Marymount International School London online community by providing a framework to promote and maintain a safe, effective and responsive online safety culture.

The policy is applicable to all members of the School. This includes governors, staff, students, volunteers, parents/carers, visitors and community users who have access to and are users of Marymount's digital technology systems both internally and externally.

### **Aims and Objectives:**

It is the duty of Marymount International School London to ensure that every student in its care is safe; and the same principles apply to the digital world as apply to the real world. Online communications and technology provide opportunities for enhanced learning, but also pose risks. Our students are therefore taught how to stay safe in the online environment and how to mitigate risks.

It is imperative that a whole school community approach to online safety is adopted and that all stakeholders are aware of their responsibilities and duties in relation to keeping children safe online. This will support a robust online safety ethos and ensure that the School is providing the best online safety provision they possibly can and identify that where there are child welfare concerns, we will take action to address them.

Technology is continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. However, many information technologies, particularly online resources, are not effectively policed. All users need to be aware, in an age-appropriate way, of the range of risks associated with the use of these internet technologies. Current and emerging technologies used in and outside of school include:

- Websites
- Email and instant messaging
- Blogs, forums and chat rooms
- Mobile internet devices such as smart phones and tablets
- Social networking sites
- Music / video / Film downloads
- Gaming sites and online communities formed via games consoles
- Instant messaging technology via SMS or social media sites

- Video calls
- Podcasting and mobile applications
- Virtual and augmented reality technology
- Artificial intelligence.

This policy, supported by the Acceptable Use Policies, is implemented to protect the interests and safety of the whole school community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements. It is linked to the following school policies and procedures:

- Safeguarding and Child Protection Policy
- Prevent Risk Assessment
- Staff Code of Conduct
- Behaviour, Rewards and Sanctions Policy
- Data Protection Policy and Privacy Notice/
- Educational Visits Policy
- RSE Policy
- Academic Honesty Policy
- Curriculum Policy
- Whistleblowing Policy<sup>1</sup>

*In producing this policy, regard has been given to:*

- |   |  |
|---|--|
| <ul style="list-style-type: none"> <li>- Department for Education (DfE) (2023) Keeping Children Safe in Education: statutory guidance for schools and colleges. London: DfE.</li> <li>- Department for Education (DfE) (2023) Teaching online safety in school: guidance supporting schools to teach their pupils how to stay safe online, within new and existing school subjects. London: DfE.</li> </ul> | <ul style="list-style-type: none"> <li>- Department for Education (DfE) (2023) Working together to safeguard children. London: DfE.</li> <li>- Department for Education (2014) Cyberbullying: Advice for headteachers and school staff. London: DfE.</li> <li>- Children Act 1989</li> <li>- Children Act 2004</li> <li>- Communications Act 2003</li> <li>- Computer Misuse Act 1990</li> <li>- Criminal Justice and Courts Act 2015</li> </ul> |
|---|--|

---

<sup>1</sup> **Disclaimer**

Every effort has been made to ensure that the information contained within this policy is up to date and accurate and reflective of the latest legislative and statutory guidance. If errors are brought to our attention, we will correct them as soon as is practicable.

- Data Protection Act 2018
- Education Act 2011
- Education and Inspections Act 2006
- Freedom of Information Act 2000
- Malicious Communications Act 1988
- Mobile phones in schools 2024
- Serious Crime Act 2015
- Voyeurism (Offences) Act 2019
- Independent School Standards Regulations 2014 (ISSR) Part 3
- General Data Protection Regulation (GDPR) 2018
- Human Rights Act 1998
- Department for Education (DfE) (2024) Mobile phones in school
- Department for Education (DfE) (2023) 'Meeting Digital and Technology Standards in Schools and Colleges' (2023)

## Scope

This policy applies to all members of the school community, including staff, students, parents and visitors, who have access to and are users of the school IT systems. In this policy:

- “staff” includes teaching and non-teaching staff, governors, and volunteers;
- “parents” includes students' carers and guardians; and
- “visitors” includes anyone else who comes to the school.

Online safety is an omnipresent topic which requires recurrent regulatory review and places a stringent duty of care on us all. Effective, timely and robust online safety is fundamental to protecting students and it is a significant part of the safeguarding agenda. The requirement to ensure that students are able to use the internet and related communication technologies appropriately and safely, is a vital part of the wider duty of care to which all who work at Marymount International School London are bound.

High quality online safety provision requires constant vigilance and a readiness to act where abuse, exploitation or neglect is suspected. Education has a vital role to fulfil in protecting students from forms of online abuse whilst demonstrating a concerted obligation to respond with haste and flexibility to concerns as they arise. Above all, all staff must foster dedication to safeguarding students, which is everyone's responsibility.

Defining online abuse: *“Online abuse is any type of abuse that happens on the web, whether through social networks, playing online games or using mobile phones”* (NSPCC, 2019).

Hidden harms – types of online abuse may include:

- Cyberbullying
- Emotional abuse
- Grooming
- Sexting

- Sexual abuse
- Sexual exploitation

The types, patterns and different circumstances of significant harm and abuse should be considered within the categories identified for children in the Children Act 1989 / 2004. These are:

- Neglect
- Sexual
- Physical
- Emotional

Technology can facilitate a world of learning and development in addition to help yield a range of opportunities. However, the stark reality is that it can also present a window to potential and actual harm and abuse. It can elicit and support an array of illegal abusive behaviours including, but not limited to:

- harassment
- stalking
- threatening and bullying behaviour
- creating or sharing child sexual abuse material
- inciting a child to sexual activity
- sexual exploitation
- grooming
- sexual communication with a child
- causing a child to view images or watch videos of a sexual act.

Whilst the use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote student achievement, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include (KCSIE 2024):

- **Content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- **Contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes’.
- **Conduct:** 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.

Many of these risks reflect situations in the off-line world and it is essential that this online safety policy is used in conjunction with other school policies such as the Behaviour and Safeguarding and Safeguarding. As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

### **Process for Monitoring the impact of the Online Safety Policy**

The School will monitor the impact of the policy using:

- Logs of reported incidents
- Filtering and monitoring logs
- Internal monitoring data for network activity
- Feedback from learners, parents/carers and staff

### **Roles and responsibilities in relation to online safety**

All staff, governors and visitors have responsibilities under the Safeguarding policy to protect children from abuse and make appropriate referrals. The following roles and responsibilities must be read in conjunction with the Safeguarding and Child Protection Policy.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the School. This may include, for example, instances of where cyber bullying has taken place over the summer holidays and has continued into term time or if a student has brought the School into disrepute over social media using a personal device, or from their home. The School will deal with such incidents within this policy and related policies, and will, where known, inform parents of incidents of inappropriate online safety behaviour that take place out of school.

### **The Governing Body**

The Governing Body has overall leadership responsibility for safeguarding as outlined in the Safeguarding and Child Protection Policy. The Governing Body of the School is responsible for the approval of this policy and for reviewing its effectiveness at least annually.

The Governing Body must ensure that their own knowledge and skill are refreshed at regular intervals to enable them to keep up-to-date with current research, legislation and trends. They must understand the unique risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online.

It should be recognised that there are additional risks online for students with SEN and disabilities (SEND), such as online bullying, grooming and radicalisation. The Governing Body must have the capability to support SEND students to stay safe online and that all students are provided with a safe environment in which to learn and develop.

The Governing Body will ensure that all staff undergo safeguarding and child protection training, both at induction and with updates at regular intervals, so that:

- all staff, in particular the DSL and Senior Leadership Team are adequately trained about online safety
- all staff are aware of the expectations, applicable roles and responsibilities in relation to filtering and monitoring and how to raise to escalate concerns when identified
- staff are aware of the school procedures and policies that should be followed in the event of the abuse or suspected breach of online safety in connection to the School
- the school has effective policies and training in place.

### **Headmistress and the Senior Leadership Team**

The Headmistress is responsible for the safety of the members of the school community and this includes responsibility for online safety. Together with the Senior Leadership Team, they are responsible for procuring appropriate filtering and monitoring systems, documenting decisions on what is blocked or allowed and why, reviewing the effectiveness of the filtering and monitoring provisions, overseeing reports and ensuring staff are appropriately trained.

### **The Designated Safeguarding Lead (DSL)**

The DSL takes the lead responsibility for Safeguarding and Child protection at Marymount International School London. This includes a responsibility for online safety as well as the School's filtering and monitoring system. The DSL must ensure that:

- they are able to understand the unique risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep students safe whilst they are online at school.
- they can recognise the additional risks that students with special educational needs and disabilities (SEND) face online, for example, from bullying, grooming and radicalisation and are confident they have the capability to support students with SEND to stay safe online.

- this policy is upheld at all times, working with the Headmistress and Senior Leadership Team/ Head of Digital Solutions and IT staff to achieve this. As such, in line with the Safeguarding and Child Protection policy, the DSL will take appropriate action if in receipt of a report that engages that policy relating to activity that has taken place online.

The DSL will work closely with the Head of Digital Solutions and the School's IT service providers to ensure that the School's requirements for filtering and monitoring are met and enforced. The DSL will review filtering and monitoring reports and ensure that checks are properly made of the system.

While the responsibility for online safety is held by the DSL and cannot be delegated, the School may choose to appoint other relevant persons to work in support of the DSL in carrying out these responsibilities.

With respect to online safety, it is the responsibility of the DSL to:

- Ensure students are being appropriately taught about and know how to use the internet responsibly.
- Ensure teachers and parents are aware of measures to keep children safe online through relevant training provision.
- Take responsibility for all safeguarding matters, including online safety.
- Collaborate with the Senior Leadership Team, the IT Managers and Computing Leads.
- Facilitate effective record keeping and the reporting and monitoring of all online safety concerns.
- Promote online safety and the adoption of a whole school approach.

### **IT Provider**

The IT service provider has technical responsibility for:

- maintaining filtering and monitoring systems
- providing filtering and monitoring reports
- completing actions following concerns or checks to systems

The IT provider should work with the Senior Leadership Team and DSL to:

- procure systems
- identify risk
- carry out reviews
- carry out checks

The Provider follows and implements School Online Safety Policy and procedures and is responsible for ensuring that;

- They are aware of and follow the School Online Safety Policy and all related policies to carry out their work effectively in line with School policy.
- The School's technical infrastructure is secure and is not open to misuse or malicious attack. Servers, wireless systems and cabling must be securely located and physical access restricted and individual workstations are protected by up to date virus software.
- The School meets (as a minimum) the required online safety technical requirements as identified by the [DfE Meeting Digital and Technology Standards in Schools & Colleges](#) and guidance from local authority / MAT or other relevant body.
- There is clear, safe, and managed control of user access to networks and devices.
- They keep up to date with online safety technical information to effectively carry out their online safety role and to inform and update others.
- The use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to the DSL.
- The filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.
- Requests from staff for sites to be removed from the filtered list will be considered by a member of SLT or Head of Digital Solutions.
- Monitoring systems are implemented and regularly updated as agreed in School policies.
- School IT technical staff regularly monitor and record the activity of users on the School ICT systems and users are made aware of this in the Acceptable Use Policy. Monitoring will take place regularly using a random sample of students.
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

### **Online Safety Committee**

The DSL will coordinate an Online Safety Committee consisting of representatives from boarding, the IT department, PSHEE department and pastoral team. They will keep up to date on current online safety issues and guidance issued by relevant organisations, including the Department for Education (including KCSIE), ISI, the CEOP (Child Exploitation and Online Protection), Childnet International and the Local Safeguarding Children Procedures. The Online Safety Committee will review the School's filtering and monitoring systems to check for patterns and make decisions about what should be blocked or permitted and will report to the Safeguarding Governor with any updates or concerns.

### **Head of Digital Solutions and IT staff**

The School's IT staff have a key role in maintaining a safe technical infrastructure at the school and in keeping abreast with the rapid succession of technical developments. They are responsible for the security of the School's hardware system, its data and for training the School's teaching and administrative staff in the use of IT. They monitor the use of the internet

and emails, maintain content filters, and will report inappropriate usage to the DSL. They ensure a robust filtering and monitoring system is in place to ensure the School's requirements are enforced. The Head of Digital Solutions works with the DSLs to investigate reports of inappropriate content being searched for or accessed within the school community.

### **Teaching and support staff**

All staff are required to sign and return the Staff Acceptable Use Policy before accessing the School's systems. Staff must also read, understand and adhere to the Staff Code of Conduct. As with all issues of safety at this school, staff are encouraged to create a culture of listening and discussion in order to address any online safety issues which may arise in classrooms on a daily basis.

All staff must read and understand all policies in school which support online safety and safeguarding and enforce these in accordance with direction from the DSL and the Headmistress / Senior Leadership Team] as appropriate.

All teachers and staff must always act in accordance with their own professional boundaries, upholding professional behaviour and conduct at all times. Staff must be aware that online conduct outside of work can impact on their professional role and responsibilities.

In addition all school staff need to:

- Support in the ownership and responsibility for the security of systems and the data accessed.
- Model good practice when using technology.
- Ensure that communication with students is on a professional level and only carried out using official school systems.
- embed all online safety issues aspects of the curriculum and other school activities.
- monitor use of IT (including AI) in lessons, extracurricular and extended school activities.
- recognise that students using mobile phones may be using their own data access and not the School's Wi-Fi.
- Know the process for making referrals and reporting concerns. All staff should self-refer any concerns regarding their use of IT systems in school.
- Know how to recognise, respond and report signs of online abuse and harm.
- Receive appropriate child protection training.
- Always act in the best interests of the child.
- Be responsible for their own continuing professional development in online safety.
- Have an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring.
- Complete up to date online safety training at least annually or more in line with legislative and statutory changes and/or online safety incidents arising.
- Check websites in advance of lessons to ensure that they are suitable.
- Be vigilant when students are allowed to freely search the internet, e.g. using approved search engines.

- Monitor students' use by monitoring and engaging with the students throughout the lesson and to be aware that students may be using mobile data to access the internet.
- Accept that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that IT temporarily remove those sites from the filtered list for the period of study. Any request to do so, should also be cleared by the DSL.
- Teach students in all lessons to be critically aware of the materials / content they access online and be guided to validate the accuracy of information, (including where the information is gained from Artificial Intelligence services).
- Teach all students to acknowledge the source of information used and to respect copyright when using material accessed on the internet. (*See Academic Honesty policy for more details.*)

## **Students**

Students are responsible for using the school IT systems in accordance with the Student Acceptable Use Policy. With respect to online safety at Marymount International School London, students need to:

- Know who the DSL is
- Engage in age appropriate online safety education opportunities
- Read and adhere to online safety policies and acceptable use agreements
- Respect the feelings of others, both off and online
- Take responsibility for keeping themselves and others safe online
- Know where and how to find help with any online incidents or concerns
- Know how, when and where to report concerns and when to seek help from a trusted adult.

Over the years at Marymount International School London, a student will cover the following topics within the curriculum:

- Self-image and identity
- Online relationships
- Online reputation
- Online bullying
- Managing online information
- Health, wellbeing and lifestyle
- Privacy and security
- Copyright and ownership

## **Parents, carers and guardians**

Marymount International School believes that it is essential for parents to be fully involved with promoting online safety both within and outside school. Parents and guardians need to

understand the risks that children face online to protect them from online dangers. Parents need to:

- Read and adhere to all relevant policies.
- Be responsible when taking photos/using technology at school events.
- Know who the school DSL is.
- Know how to report online issues.
- Support online safety approaches and education provision.
- Be a role model for safe and appropriate behaviour.
- Identify changes in children's behaviour that could indicate they are at risk of online harm or abuse.
- Take responsibility for the filtering, monitoring and regulating of their own IT systems at home.

The school will contact parents if it has any concerns about students' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the School.

The school recognises that not all parents and guardians may feel equipped to protect their child when they use electronic equipment at home. The school therefore arranges discussion evenings for parents when an outside specialist advises about online safety and the practical steps that parents can take to minimise the potential dangers to their children without curbing their natural enthusiasm and curiosity.

#### MONITORING AND FILTERING OF DIGITAL AND TECHNOLOGY SYSTEMS

At Marymount International School, Governors, SLT and the Head of Digital Solutions work together to provide a safe environment to learn and work, including when online. Filtering and monitoring are both important parts of safeguarding students and staff from potentially harmful and inappropriate online material.

The school manages access to content across its systems for all users and on all devices using the schools internet provision. The filtering provided meets the standards defined in the DfE Filtering standards for schools and colleges. Illegal content is filtered by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated.

Filtering logs are regularly reviewed and alert the Designated Safeguarding Lead to breaches of the filtering policy, which are then acted upon. There are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective. These are acted upon in a timely manner.

There are regular checks of the effectiveness of the filtering systems . Checks are undertaken across a range of devices at least termly and the results recorded and analysed to inform and improve provision. The DSL and Governor are involved in the process and aware of the findings.

The School has monitoring systems in place to protect the School, systems and users. The school monitors all network use across all its devices and services. Monitoring reports are urgently picked

up, acted on and outcomes are recorded by the Designated Safeguarding Lead, all users are aware that monitoring is in place. There are effective protocols in place to report abuse/misuse and alerts that require an urgent response are done so swiftly for safeguarding interventions in accordance with safeguarding policy and practice.

## RESPONSIBILITY AND ALLOCATION OF TASKS

The Board of Governors has overall strategic responsibility for filtering and monitoring. To ensure the efficient discharge of its responsibilities under this policy, the Board of Governors has allocated the tasks:

Task/ Responsibility	Allocated to	When/Frequency of Review
<ul style="list-style-type: none"> <li>• Procuring filtering and monitoring systems</li> </ul>	Bursar & Head of Digital Solutions	Annual
<ul style="list-style-type: none"> <li>• Documenting decisions on what is blocked or allowed and why</li> </ul>	DSL / Head of Digital Solutions	Termly or as required
<ul style="list-style-type: none"> <li>• <b>Reviewing</b> the effectiveness of the School’s provision in order to:               <ul style="list-style-type: none"> <li>○ identify risk</li> <li>○ carry out reviews</li> <li>○ carry out checks</li> <li>○ inform practice and procedures</li> </ul> <p>The review should indicate:</p> <ul style="list-style-type: none"> <li>○ the risk profile of the student body, including their age range, students with special educational needs and disability (SEND), students with English as an additional language (EAL)</li> <li>○ what the filtering system currently blocks or allows and why</li> <li>○ any outside safeguarding influences</li> <li>○ any relevant safeguarding reports</li> <li>○ the digital resilience of the students</li> </ul> </li> </ul>	SLT DSL Head of Digital Solutions (in collaboration with any external provider – e.g. Smoothwall / Zed One) Cristina Serrano (Governor) Niamh Green (Governor)	Annual report (or if a safeguarding risk is identified / there is a change in working practice / new technology is introduced)

<ul style="list-style-type: none"> <li>○ teaching requirements in RSE and PSHEE</li> <li>○ the specific use of chosen technologies, including Bring Your Own Device (BYOD)</li> <li>○ related safeguarding or technology policies</li> <li>○ current checks and how actions are handled</li> </ul>		
<ul style="list-style-type: none"> <li>• Overseeing reports</li> </ul>	Headmistress	Annual
<p>Oversight of all staff to ensure they:</p> <ul style="list-style-type: none"> <li>• understand their role</li> <li>• are appropriately trained</li> <li>• follow policies, processes and procedures</li> <li>• act on reports and concerns</li> </ul>	SLT	Training at annual induction and ongoing oversight
<ul style="list-style-type: none"> <li>• Overseeing and acting on: <ul style="list-style-type: none"> <li>- filtering and monitoring reports</li> </ul> </li> </ul>	DSL and Head of Digital Solutions (Staff)  HOYs/DSL and Head of Digital Solutions – (Students)	Bi-weekly or as required
<ul style="list-style-type: none"> <li>• Overseeing and acting on: <ul style="list-style-type: none"> <li>• safeguarding concerns</li> </ul> </li> </ul>	DSL	As required
<ul style="list-style-type: none"> <li>• Overseeing and acting on: <ul style="list-style-type: none"> <li>• checks to filtering and monitoring systems</li> </ul> </li> </ul> <p>(Checks to be recorded to include date, person who checked, what was checked and resulting action)</p>	DSL / Head of Digital Solutions	Termly or as required
<p>Technical responsibility for:</p> <ul style="list-style-type: none"> <li>• maintaining filtering and monitoring systems</li> </ul>	Head of Digital Solutions	Ongoing
<p>Technical responsibility for:</p> <ul style="list-style-type: none"> <li>• Providing filtering and monitoring reports</li> </ul>	Head of Digital Solutions	Ongoing

Technical responsibility for: <ul style="list-style-type: none"> <li>• completing actions following concerns or checks to systems</li> </ul>	Head of Digital Solutions	Ongoing
Responsibility for ensuring: <ul style="list-style-type: none"> <li>• there is an appropriate level of security protection procedures in place in order to safeguard systems, staff and learners</li> <li>• Review of the effectiveness of these procedures periodically to keep up with evolving cyber-crime technologies</li> </ul>	Head of Digital Solutions	Annual or as required

### Cultivating a safe environment

The online world develops and changes at a great speed. New opportunities, challenges and risks are appearing all the time. This can make it difficult for schools to stay up to date with the latest devices, platforms, apps, trends and related threats.

It is important to focus on the underpinning knowledge and behaviours that can help students to navigate the online world safely and confidently regardless of the device, platform or app. This teaching could be:

- built into existing lessons across the curriculum
- covered within specific online safety lessons
- covered using school-wide approaches (Teaching online safety in schools 2023)

Students should be educated in an age-appropriate way around:

- How to evaluate what they see online
- How to recognise techniques for persuasion
- Their online behaviour
- How to identify online risks
- How and when to seek support

- **Evaluate: How to evaluate what they see online**

This will enable students to make judgements about what they see online and not automatically assume that what they see is true, valid or acceptable.

Through the curriculum, students will consider questions including:

- Is this website/URL/email fake? How can I tell?
- What does this cookie do and what information am I sharing?
- Is this person who they say they are?
- Why does someone want me to see this?
- Why does someone want me to send this?
- Why would someone want me to believe this?

- **Recognise: How to recognise techniques used for persuasion**

This will enable students to recognise the techniques that are often used to persuade or manipulate others. A strong grasp of knowledge across many areas makes people less vulnerable to these techniques and better equipped to recognise and respond appropriately to strongly biased intent or malicious activity.

Students will be encouraged to question content so that they are able to recognise:

- Online content which tries to make people believe something false is true and/or mislead (misinformation and disinformation).
- Techniques that companies use to persuade people to buy something.
- Ways in which games and social media companies try to keep users online longer
- Criminal activities such as grooming.

- **Online Behaviour**

Students will consider what acceptable and unacceptable online behaviour looks like. Students must recognise that the same standard of behaviour and honesty applies online and offline, including the importance of respect for others. Students should also be able to recognise unacceptable behaviour in others.

The School will help students to recognise acceptable and unacceptable behaviour by:

- Looking at why people behave differently online. For example, how anonymity (you do not know me) and invisibility (you cannot see me) affect what people do.
- Looking at how online emotions can be intensified resulting in mob mentality.
- Teaching techniques (relevant on and offline) to defuse or calm arguments (for example, a disagreement with friends) and disengage from unwanted contact or content online; and
- Considering unacceptable online behaviours often passed off as so-called social norms or just banter. For example, negative language that can be used, and in some cases is often expected, as part of online gaming and the acceptance of misogynistic, homophobic and racist language that would never be tolerated offline.

- **Identify: How to identify online risks**

This will enable students to identify possible online risks and make informed decisions about how to act. The focus should be to help students assess a situation, think through the consequences of acting in different ways and decide on the best course of action.

Students will be taught to identify and manage risk by:

- Discussing the ways in which someone may put themselves at risk online.
  - Discussing risks posed by another person's online behaviour.
  - Discussing when risk taking can be positive and negative.
  - Discussing "online reputation" and the positive and negative aspects of an online digital footprint. This could include longer-term considerations; i.e. how past online behaviours could impact on their future when applying for a place at university or a job for example.
  - Discussing the risks vs the benefits of sharing information online and how to make a judgement about when and how to share and who to share with.
  - Asking questions such as what might happen if I post something online? Who will see it? Who might they send it to?
- **How and when to seek support**

Students will consider safe ways in which to seek support if they are concerned or upset by something they have seen online.

Staff will help students to:

- To identify who trusted adults are.
- Look at the different ways to access support from the school, police, the National Crime Agency's Click CEOP reporting service for children and 3rd party organisations, such as Childline and the Internet Watch Foundation. This links to wider school policies and processes around reporting of safeguarding and child protection incidents and concerns to school staff.
- To understand that various platforms and apps will have ways in which inappropriate contact or content can be reported and/or blocked.

## **Responding to Online Safety Concerns**

The safety of the student is of paramount importance. Immediate action may be required to safeguard investigations and any other students. Any concern that a child may be at risk of harm or abuse must immediately be reported.

Online safety is recognised as part of the safeguarding responsibilities – the DSL should take lead responsibility for online safety concerns which should be recorded and actioned. Students can share concerns and report online safety concerns to a trusted adult such as their Advisor, Head of Year, School Counsellor or a member of the DSL team. Students can also report using the worry boxes or the Teams Chat function or email.

It is assumed that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Any such incidents should be reported to the DSL. All staff are reminded that there is a clear school Whistleblowing policy.

**Remember:**

- Child welfare is of principal concern – the best interests of children take precedence.
- If there is any immediate danger, contact the police on 999.
- Staff need to notify the DSL team
- Use CEOP's or KRSCP's processes if it requires.
- Always adhere to local safeguarding procedures and report to the DSL and/or Headmistress.

### **Use of school and personal devices including mobile phones**

#### **Staff**

School devices assigned to a member of staff as part of their role must have a password or device lock so that unauthorised people cannot access the content. Staff should only use the school device which is allocated to them for school work. When they are not using a device staff should ensure that it is locked to prevent unauthorised access.

Staff are referred to the Staff Code of Conduct and IT Acceptable Use Policy for further guidance.

Staff are not permitted under any circumstances to use their personal devices when taking images, videos or other recording of any student nor to have any images, videos or other recording of any student on their personal devices. Please read this in conjunction with Safeguarding and Child Protection, Acceptable Use Policy, Staff Code of Conduct and School Educational Visits policies.

#### **Students**

Phone use is not seen as necessary for the education of students at the School and students are discouraged from bringing a phone on to campus. Should a student choose to take a mobile device on to the school campus, they are responsible for any loss or damage to the device.

The School understands the need for students to learn how to self-regulate their use of technology as they become an adult. A graduated approach has therefore been adopted for students as they progress throughout the School (see below).

For all students mobile devices are not permitted in the Dining Hall during the school day.

Should students wish to contact their parents or guardian during the school day, students should use the school phones in the Reception area. Parents or guardians can leave a message at Reception if there is an urgent need to contact the student. Parents are not permitted to collect their daughter from the school if they are feeling unwell without prior permission from the Nurse. (*Please see Medical Health and Wellbeing Policy*).

### **Grades 6-10:**

If students bring in mobile devices (e.g. for use during the journey to and from school), they should be switched off and handed in to Reception at the start of the day and collected as they leave school. These requirements apply to phones and all devices that communicate over the internet, including smartwatches and other wearable technology. Boarders in Grades 6-10 must leave all personal devices in their rooms during the school day.

At the Headmistress's discretion, Grade 10 may be permitted the same privilege as Grades 11 and 12 following Spring Break of their MYP Programme. This will, however, be dependent on the conduct and behaviour of the whole Grade throughout the year. Grade 10 Representatives will have to apply to the Headmistress, in writing, to request use of their mobile devices.

### **Grades 11-12:**

Students in Grades 11 and 12, are permitted access to devices but these must be switched off during the school day unless during a breaktime, lunchtime or study period. They must only be used in the DP Lounge (Grade 12) or free classroom (Grade 11) at these times. Students in Grades 11 and 12 are expected to be role models for the younger students and should not use their mobile devices on the school paths or in the school gardens.

### **Boarding**

In Boarding, students are permitted to use their mobile devices but efforts are made to monitor their usage in the following ways:

Grades 6 – 9 must hand in all devices 30 minutes prior to bed time on Sunday-Thursday. During Supervised Study, Grades 6-9 are allowed to use their phones to listen to music but not to contact others. If it seems the phone is a distraction to their study, the Boarding team will remove the phone.

Grade 10 will have supervised study and will not be permitted to use their mobile phones in the First Semester. At the Head of Boarding's discretion, students can apply to the Head of Boarding to have study in their rooms in the Second Semester. Students will be encouraged to switch off their devices during study time.

Grades 11-12 have private study in their own rooms and have access to their mobile devices. They are encouraged to self-regulate their use of their devices and develop good habits.

No use of mobile phones in the Dining Hall during all meal times.

## **Laptops and Tablets**

The School expects that all students will own a laptop as a teaching and learning tool and students are required to adhere to the Student Acceptable Use Policy when using tablets or laptops for school work. In particular, the Student Acceptable Use Policy requires students to ensure that their use of tablets for school work complies with this policy and the Student Acceptable Use Policy which prohibits students from using tablets for non-school related activities during the school day.

School mobile technologies are made available for student use by the School (including laptops, tablets, cameras, etc.) which are stored in the IT office or Art/Design office. Access is available via the Head of Digital Solutions. Members of staff should sign devices out and in before and after each use by a student. Students are responsible for their conduct when using school issued or their own devices. Any misuse of devices by students will be dealt with under the School's Behaviour, Rewards and Sanctions Policy.

The school recognises that mobile devices are sometimes used by students for medical purposes or as an adjustment to assist students who have disabilities or special educational needs. Where a student needs to use a mobile device for such purposes, the student's parents, carer or guardian should arrange a meeting with the student's Head of Year or Learning Resources teacher to agree how the School can appropriately support such use. The Head of Year or Learning Resources Teacher will then inform the student's teachers and other relevant members of staff about how the student will use the device at school.

## **Online Communications**

### **Staff**

Any digital communication between staff and students or parents / carers /guardians must be professional in tone and content. Under no circumstances may staff contact a student or parent / carer / guardian or recent alumni (i.e. students over the age of 18 who have left the school within the past 5 years or parents of recent alumni using any personal email address or SMS / WhatsApp / social media. *(Students may contact staff via LinkedIn after 3 years of graduating from School. Please see Staff Code of Conduct and Staff Acceptable Use Policies for further details.)*

The School ensures that staff have access to their work email address when offsite, for use as necessary on school business. Personal telephone numbers, email addresses, or other contact details, may not be shared with students or parents / carers /guardians or recent alumni. Under no circumstances may staff contact a student or parent / carer /guardian or recent alumni using a personal telephone number, email address, or other messaging system nor should students, parents / carers / guardians or recent alumni / their parents / carers] be added as social network 'friends' or similar.

Staff must immediately report to the DSL or Headteacher the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication. Staff must remain alert to the risk of fraudulent emails and should report emails they suspect to be fraudulent to Head of Digital Solutions.

## **Students**

All students are issued with their own personal school email addresses for use on our network [and by remote access]. Access is via a personal login, which is password protected. This official email service may be regarded as safe and secure, and must be used for all schoolwork. Students should be aware that email communications through the school network and school email addresses are monitored.

The School will ensure that there is appropriate and strong IT monitoring and virus software. Spam emails and certain attachments will be blocked automatically by the email system. If this causes problems for school purposes, students should contact Head of Digital Solutions for assistance.

Students must not respond to any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and should immediately report such a communication, to a member of staff who should then refer it to the DSL.

## **Use of social media**

### **Staff**

Staff must not access social networking sites, personal email or any website which is unconnected with school work or business from school devices or whilst teaching / in front of students. Such access may only be made from staff members' own devices whilst in staff-only areas of school.

When accessed from staff members' own devices and /or off school premises, staff must use social networking sites with extreme caution, being aware of the nature of what is published online and its potential impact on their professional position and the reputation of the School in accordance with the Staff Code of Conduct.

Any online communications, whether by email, social media, private messaging or other, must not:

- place a child or young person at risk of, or cause, harm;
- bring Marymount International School London into disrepute;
- breach confidentiality;
- breach copyright;
- breach data protection legislation;

- or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
  - making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
  - using social media to bully another individual; or
  - posting links to or endorsing material which is discriminatory or offensive.
- otherwise breach the Staff Code of Conduct or Safeguarding and Child Protection Policy.

## **Students**

The School expects students to think carefully before they post any information online, or repost or endorse content created by other people. Content posted must not be, or potentially be, inappropriate or offensive, or likely to cause embarrassment to an individual or others. The school takes misuse of technology by students very seriously and incidents will be dealt with under the Behaviour, Rewards and Sanctions Policy, Student Acceptable Use Policy, Safeguarding and Child Protection and Anti-Bullying policies as appropriate.

## **Data protection**

Please refer to the Data Protection policy and the Staff Acceptable Use Policy for further details as to the key responsibilities and obligations that arise when personal information, particularly that of children, is being processed by or on behalf of the School.

Staff and students are expected to save all data relating to their work to their school's OneDrive.

Staff devices should be encrypted if any data or passwords are stored on them. The school expects all removable media (USB memory sticks, CDs, portable drives) taken outside school or sent by post or courier to be encrypted before sending.

Staff may only take information offsite when authorised to do so, and only when it is necessary and required in order to fulfil their role. No personal data of staff or students should be stored on personal memory sticks, but instead stored on an encrypted USB memory stick provided by the school.

Staff should also be particularly vigilant about scam / phishing emails (and similar) which could seriously compromise the school's IT security and/or put at risk sensitive personal data (and other information) held by the School. If in any doubt, do not open a suspicious email or attachment and notify the Head of Digital Solutions in accordance with the Data Protection Policy and Acceptable Use Policies.

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the Head of Digital Solutions.

### **Password security**

Students and staff have individual school network logins and storage folders on the server. Staff and students are regularly reminded of the need for password security.

The UK National Cyber Security Centre recommends three random words for passwords. Marymount expects students and staff to use this advice, adding special characters and numbers to strengthen the password. The password should be at least 12 characters long.

All students and members of staff should:

- use a strong password (as described above) which should be changed every 6 months;
- not write passwords down; and
- not share passwords with other students or staff;
- Immediately report any suspicion or evidence that there has been a breach of security.

Care will be taken when using Artificial Intelligence services to avoid the input of sensitive information, such as personal data, internal documents or strategic plans, into third-party AI systems unless explicitly vetted for that purpose. Staff must always recognise and safeguard sensitive data. and use dual-factor authentication, where possible, for sensitive data or access outside of a trusted network.

### **Safe use of digital and video images**

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying, stalking or grooming to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. Employers are likely to carry out internet searches for information about potential and existing employees.

When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

Staff are allowed to take digital / video images to support educational aims but must follow the School's policy (Safeguarding and Child Protection policy and Staff Code of Conduct) concerning the sharing, distribution and publication of those images. Those images should be

taken on school equipment; the personal equipment of staff should not be used for such purposes. If a member of staff wants to use their own equipment they need the permission of the Deputy Head Pastoral.

Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the School into disrepute. If in doubt, the individual should ask the advice from a member of SLT.

Students must not take, use, share, publish or distribute images of other students without their permission. It must be recognised by the students that these permissions can change depending on the relationship between particular groups of students.

Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images. The School's Term and Conditions clarifies what is permissible and parents are required to give consent for the sharing of such images when signing the school contract. Any images which are published should be without the full name of the individual student (unless permission has been agreed by the student and their parent).

Particular care should be taken in subjects such as Art, where it may be necessary for students to capture images using digital media of semi-naked models as part of their portfolio work. Advice should be sought from the DSL for safeguarding if there are any concerns.

## **Artificial Intelligence**

**The School acknowledges the potential benefits of the use of AI in an educational context – including** enhancing learning and teaching, improving outcomes, improving administrative processes, reducing workload and preparing staff and learners for a future in which AI technology will be an integral part. The School/Staff will comply with all relevant legislation and guidance, with reference to guidance contained in KCSIE and UK GDPR. Staff must ensure that tools meet data security standards before using them for work related to the School.

- AI incidents must be reported promptly. Staff must report any incidents involving AI misuse, data breaches, or inappropriate outputs immediately to the Deputy Head Academic/ Bursar/ DSL.
- The school will audit all AI systems in use and assess their potential impact on staff, learners and the School's systems and procedures, creating an AI inventory listing all tools in use, their purpose and potential risks.
- When procuring and implementing AI systems, we will follow due care and diligence to prioritise fairness and safety to reduce discrimination and bias that may be a potential risk from AI tools.
- The school will support parents in their understanding of the use of AI in the school
- AI tools may be used to assist teachers in the assessment of learners' work, identification of areas for improvement and the provision of feedback. Teachers may also support learners to gain feedback on their own work using AI.

Any usage by students of generative AI tools such as ChatGPT is only permitted in the circumstances outlined in the Academic Honesty Policy and are subject to any conditions imposed by that policy. Staff will seek to support learners to understand how AI works, its potential benefits, risks and impacts and help equip learners with the knowledge, skills and strategies to engage responsibly with AI tools.

Personal or confidential information should not be entered into generative AI tools. This technology stores and learns from data inputted and you should consider that any information entered into such tools is released to the internet. Although paid-for versions of AI may offer assurances that no input data will be used externally or for training the tool, such assurance should be approached with caution.

It is also important to be aware that the technology, despite its advances, still produces regular errors and misunderstandings and should not be relied on for accuracy. In particular, students should not use these tools to answer questions about health / medical / wellbeing issues, or indeed anything of a personal nature. It is always best to seek help and recommendations as to reliable resources from a member of staff / DSL team.

## **Misuse**

Marymount International School London will not tolerate illegal activities or activities that are in breach of the policies referred to above. Where appropriate the School will report illegal activity to the police and/or the local safeguarding partnerships. If a member of staff discovers that a child or young person is at risk as a consequence of online activity they should report it to the DSL. The DSL then may seek assistance from the CEOP, the LADO, KRSCP, and/or its professional advisers as appropriate.

The School will impose a range of sanctions on any student who misuses technology to bully, harass or abuse another student in line with our Safeguarding and Child Protection, Anti-Bullying and Behaviour, Rewards and Sanctions policies.

## **Cyber Security**

The School is aware of the risks and impact of cyber security attacks and has reviewed the DfE Cyber Security standards. A risk assessment is in place which is reviewed annually or as required. The School has an effective backup and restoration plan in place in the event of cyber attacks. Training on cyber security is delivered to staff and governors and the School's PSHEE curriculum helps learners with cyber awareness.

All students and staff have a responsibility to report cyber risk or a potential incident or attack to the Head of Digital Solutions.

## **Training**

All staff are trained in online safety through the School CPD Programmes. Useful resources for online safety to inform governors, staff, parents and students can be found in Annex B of KCSIE. Resources are also shared with staff via SharePoint / CPD, with parents via the Parent Portal or email, newsletters and guest speakers, and with students through the Advisor and PSHEE curricula, whole school assemblies, as well as being embedded in the teaching and learning of the curriculum. All staff are provided with information to help inform their understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring systems in the school.

Governors with oversight for Online Safety and IT also receive training on cybersecurity and the monitoring and filtering systems in the school.

## **Complaints**

As with all issues of safety at the School, if a member of staff, a student or a parent / carer / guardian has a complaint or concern relating to online safety, prompt action will be taken to deal with it.

Who to see if you have a complaint:

- Students should speak to their Head of Year.
- Staff should speak to their Line Manager or member of the SLT/Headmistress.
- Parents should refer to the Complaints Policy.

Incidents of, or concerns around online safety will be recorded in accordance with the Safeguarding and Child Protection policy.

**Approved:                    May 2025**

**Reviewed:**

**Next Review By:    May 2028**