

2026/2027

E-Safety and Electronic Devices Policy

WHOLE SCHOOL

Owned By:
Head Teacher



SINCE 1973

1. Purpose and Scope

Morna International College is committed to the safe, responsible and healthy use of technology. This policy is the school's principal policy for online safety and electronic devices and sets enforceable expectations for students, staff, parents and carers, visitors and other members of the school community.

For the purposes of this policy, "online safety" means the safeguarding, responsible-use and security arrangements applying to digital technology, online services, electronic communications, accounts and devices. The term "e-safety" is retained in the policy title for continuity but has the same meaning as "online safety" within this policy and related school documents. The policy covers school-owned and personal devices, networks, accounts, cloud services, online communication, generative AI, images and recordings, cybersecurity, data protection and mobile phones. It also applies to off-site online behaviour where there is a connection with the school or an impact on the safety, wellbeing, reputation or learning of the school community.

This policy must be read alongside the Safeguarding and Child Protection Policy, Behaviour Policy, Anti-Bullying Policy, Privacy & Data Protection Policy, Staff Code of Conduct and Morna Community Code, together with the Acceptable Use Agreements listed in section 15. Where a safeguarding concern is identified, safeguarding procedures take priority.

2. Key Online Risks

The school seeks to protect students from harmful or inappropriate content, including pornography, violence, hate speech, extremism, self-harm content and misinformation; grooming, exploitation, sextortion and online sexual harassment; cyberbullying, impersonation, identity theft and unsafe sharing of personal information or images; nude or semi-nude imagery, deepfakes and harmful AI-generated content; scams, phishing, hacking, malware and compromised accounts; excessive screen time, gambling and harmful online challenges; plagiarism, copyright breaches and misuse of generative AI; and attempts to bypass school controls through VPNs, hotspots, proxies or similar methods.

3. Roles and Responsibilities

The Head Teacher is the policy owner and is operationally accountable for implementation of this policy. The Head Teacher ensures that online-safety expectations are embedded in teaching, behaviour, staff practice and communication with families; that staff receive appropriate training; that Acceptable Use Agreements are issued and reviewed; and that serious or repeated breaches are addressed consistently.

The Executive Director provides strategic oversight and assurance but does not replace the Head Teacher's operational accountability for implementation. The Executive Director ensures that appropriate resources and oversight arrangements are in place and is informed of significant cyber incidents, serious data breaches, major failures of filtering or monitoring, and other incidents that create material risk to the school.

The IT Team has technical responsibility for the security and operation of school networks, accounts and managed devices. It maintains filtering, monitoring, device-management, access-control, backup and security measures; investigates technical alerts and cyber incidents; preserves relevant technical evidence; supports containment and recovery; and escalates safeguarding or data-protection concerns to the appropriate lead.

Designated Safeguarding Leads (DSLs) have safeguarding responsibility for online concerns involving children, including grooming, exploitation, sextortion, sexual imagery, harmful deepfakes, harassment,

radicalisation or other online harm. DSLs decide safeguarding actions, recording, parent/carer contact and external referrals in accordance with the Safeguarding and Child Protection Policy.

Teaching staff and other staff are responsible for appropriate supervision, age-appropriate use of digital resources, compliance with the Staff Code of Conduct and Staff Acceptable Use Agreement, protection of confidential information, and prompt reporting of safeguarding, technical or data-protection concerns. Staff must not investigate safeguarding incidents beyond what is necessary to establish and report the concern.

Students must use technology safely, responsibly and respectfully; protect passwords and personal information; comply with the Student Acceptable Use Agreement and mobile phone-free rules; and report concerns promptly.

Parents and carers are expected to support the school's online-safety expectations and to take responsibility for the appropriate supervision and management of their child's use of technology outside school hours, as set out in section 6. They should use the school office for urgent contact during the school day and comply with the mobile-phone rule within the school perimeter fence, as set out in section 10.

4. Safe Use of Technology and School Systems

School internet access should normally use the approved network, and online resources used in lessons must be relevant, age-appropriate and consistent with teacher instructions. Users must not bypass, disable or interfere with filtering, monitoring, device-management or security controls, including through VPNs, personal hotspots, proxies or unauthorised software.

School-managed devices must be used in accordance with school rules and the relevant Acceptable Use Agreement. Secondary students must use school-approved, school-managed laptops unless an exception is authorised. Smartwatches and other wearables must not be used for messaging, calling, recording or internet access during the school day unless an authorised medical or other exceptional arrangement applies.

School information must be created, stored and shared through approved school systems. Users must not transfer confidential or sensitive school information to personal accounts, unauthorised cloud services, removable media or unapproved applications.

5. Online Safety Education

Through PSHE, ICT/Computing and other relevant subjects, students will learn to assess online information critically; recognise misinformation, bias and deepfakes; communicate safely and respectfully; protect privacy, passwords and digital reputation; identify grooming, exploitation, sextortion, cyberbullying and harassment; report concerns; use images, recordings, online content and generative AI safely and lawfully; recognise scams, phishing and cybersecurity risks; and develop healthy screen habits.

Staff will receive induction and periodic guidance appropriate to their role. Data-protection training is provided, and filtering and monitoring and cybersecurity are addressed through the school's wider safeguarding and IT arrangements. Updated safeguarding training through Tes Develop includes AI and safeguarding/responsible use and will be completed by all staff. Training and guidance will be reviewed and updated as appropriate to reflect emerging risks and school practice. Parents and carers will be provided with appropriate information to reinforce safe technology use at home.

6. Parental Responsibility and Online Safety Outside School Hours

Parents and carers have primary responsibility for supervising and managing their child's use of personal devices, internet access, social media, messaging services, gaming platforms and other online services outside school hours.

The school strongly encourages parents and carers to establish age-appropriate boundaries for screen time, applications, social media, online communication and access to online content, and to make appropriate use of parental controls and filtering tools.

To support families, Morna International College provides access to Qustodio in connection with students' school-managed devices. Outside school hours, parents and carers can use Qustodio to manage appropriate controls and filtering on the school-managed device. The school also currently provides families with the facility to protect one additional personal device per student. Guidance on registration and configuration is provided in Annex 1 – Qustodio Family Quick Guide

7. Generative AI

AI may be used only when appropriate to the learning task and teacher instructions. Students must not submit AI-generated work as their own or use AI to bypass assessment requirements, and AI use must be acknowledged where required. Confidential, sensitive or personal school information must not be entered into unapproved AI systems, and AI-generated information must be checked critically.

AI must never be used to create abusive, deceptive, discriminatory, sexualised or harmful content. Harmful deepfakes or manipulated images will be treated as serious misconduct and, where relevant, a safeguarding matter. Any suspected harmful AI-generated imagery involving a student must be handled under the harmful imagery procedure in section 12.

8. Accounts, Cybersecurity and Lost Devices

Passwords must remain confidential and users must not access another person's account. Multi-factor authentication must be used where required. Suspected phishing, malware, compromised accounts or unauthorised access must be reported immediately to the IT Team. The user should stop interacting with the suspicious message or system and follow IT instructions; passwords must be changed promptly where directed.

Any school-managed device, or personal device authorised to hold or access school information, that is lost or stolen must be reported immediately to the IT Team and to the user's line manager or relevant teacher. The report should state when and where the device was last seen and whether it may contain or provide access to personal or confidential information. Where personal or confidential information may be accessible, the incident must also be treated as a suspected data breach under section 9. The IT Team will take proportionate action, which may include account suspension, password resets, remote locking or wiping where technically possible, preservation of relevant logs, and assessment of whether further security or data-protection action is required.

For a significant cyber incident, the IT Team leads technical containment, evidence preservation, recovery and security actions; the Head Teacher coordinates educational and operational decisions; DSLs lead any child-safeguarding response; and the Executive Director is informed where the incident is serious or materially affects school operations, data or reputation. Users must not conduct their own technical investigation, delete evidence or communicate externally about an incident unless authorised.

9. Data Protection and Suspected Data Breaches

Personal data must be handled in accordance with the Privacy & Data Protection Policy. Sensitive information must be shared only where necessary, through approved systems and with authorised recipients. Personal information or images must not be published without appropriate permission or another lawful basis.

A suspected data breach includes loss, accidental disclosure, misdirected email, unauthorised access, compromised credentials, loss of a device containing personal data, or any other incident that may affect the confidentiality, integrity or availability of personal data. Staff must report a suspected breach immediately to the Finance & Business Support Officer, who is responsible for the day-to-day administration of data protection matters. The Head Teacher should also be informed where the incident involves operational or educational matters, and the IT Team must be notified where technical systems or accounts are involved.

The Finance & Business Support Officer will ensure that the incident is recorded, contained and assessed in accordance with the Privacy & Data Protection Policy, including any required notification or escalation to the Executive Director, as the School's Legal Representative. Staff must not conceal, independently investigate or contact affected individuals about a suspected breach unless instructed to do so.

10. Mobile Phone-Free School and Campus Expectations

Morna International College is a mobile phone-free school for all students, including Years 12 and 13. Mobile phones must not be used by students within the school perimeter fence during the school day, unless a specific exception has been authorised. This applies during lessons, registration, breaks, lunch and movement between lessons. Parents and carers should contact students through the school office, while students needing to contact home should seek staff assistance.

Staff, parents, carers and visitors are expected to keep personal mobile phones out of sight and not use them within the school perimeter fence during school hours, except where use is required for an emergency, an agreed medical need, an authorised safeguarding or operational purpose, or another necessary circumstance approved by the school. Staff use of any personal device must also comply with the Staff Code of Conduct, the Staff Acceptable Use Agreement and section 11 of this policy. Parents and carers should also refer to the Parent/Carer Community Code for further details of the school's expectations.

Unauthorised student use of a mobile phone, smartwatch or other personal electronic device will normally result in confiscation until at least the end of the school day, subject to safeguarding, medical, disability-related or other exceptional circumstances. A confiscated device will be transferred promptly to the relevant Head of Section or the Head Teacher, recorded and kept securely in a locked office. The school will take reasonable care of confiscated devices but is not responsible for pre-existing damage or for loss arising from a student's failure to follow the handover procedure.

For a first or minor breach, the device will normally be returned to the student at the end of the school day. For repeated breaches, the school may retain the device for longer and may require collection by a parent, carer or other authorised adult. The school will notify the parent or carer where a device is to be retained beyond the end of the school day and advise them of the collection arrangements.

Repeated, concealed or defiant breaches may lead to further sanctions under the Behaviour Policy. Misuse involving filming, bullying, harassment, threats, sexual or harmful content, or evidence relevant to safeguarding will be referred to a DSL and may result in the device being retained or handled differently

where necessary to protect a child or preserve evidence. Staff must not search the content of a confiscated phone unless specifically authorised and permitted under applicable school procedures. Medical, disability-related or other exceptional exemptions must be agreed in advance and recorded.

11. Staff Use of Personal Devices

Staff should use school-managed devices and approved school systems for school business wherever provided. Personal devices must not be used to photograph, film or record students, access or store confidential student information, or conduct routine school communication unless there is an expressly authorised school procedure that permits this.

Where exceptional use of a personal device is authorised for a necessary school purpose, the minimum amount of information must be used, it must be transferred to the approved school system as soon as practicable, and any local copy must then be securely deleted. Personal messaging accounts and personal social-media accounts must not be used to communicate privately with students. All staff use remains subject to the Staff Code of Conduct, Privacy & Data Protection Policy and Staff Acceptable Use Agreement.

12. Images, Recording and Harmful Imagery

Students must not photograph, film or record others, lessons, meetings or conversations without authorisation. Educational images and recordings must be captured, stored and shared only through approved arrangements, and external publication requires appropriate authorisation.

Any concern involving nude or semi-nude imagery of a student, sexualised deepfakes, coercive image-sharing, sextortion or potentially illegal imagery must be reported immediately to a DSL. Staff and students must not ask for the image to be sent to them, must not forward or copy it, and must not unnecessarily view, save, print or screenshot it. The DSL will follow the school's safeguarding procedure, record decisions, consider parent/carer contact and external referral, and ensure that any evidence is preserved only in a safe and proportionate manner.

Where an image or recording is also evidence of bullying, harassment, threats or another behaviour incident, the safeguarding response takes priority where there is a risk of harm. Device confiscation or access decisions must be made in consultation with a DSL where harmful imagery may be present.

13. Filtering and Monitoring Alerts

The school uses filtering and monitoring systems as part of its safeguarding and cybersecurity controls. The IT Team is responsible for maintaining the technical systems. Alerts are reviewed through a combination of IT Support and the relevant pastoral leaders, depending on the nature of the alert. Filtering and monitoring do not replace staff supervision.

Alerts indicating possible safeguarding risk, harmful content, attempts to bypass controls, compromised accounts or unusual activity must be reviewed promptly according to their severity. IT Support will address technical issues and preserve relevant logs where appropriate. Where an alert may indicate risk to a child, it must be escalated without delay to a DSL or appropriate safeguarding lead in line with the school's safeguarding procedures. Repeated or deliberate attempts to circumvent controls must also be reported to the Head Teacher or relevant pastoral/behaviour lead.

Actions and outcomes arising from alerts will be recorded through the appropriate IT, pastoral and/or safeguarding process, according to the nature of the concern. Staff reviewing alerts must avoid

unnecessary access to harmful material and must not copy or circulate such material except where specifically required by an authorised safeguarding or technical process.

14. Reporting, Recording and Incident Response

Safeguarding concerns must be reported immediately to a DSL. Cybersecurity concerns must be reported promptly to the IT Team. Suspected data breaches must be reported through the route in section 9. Where an incident falls into more than one category, the relevant leads must coordinate their response rather than treating the matter in isolation.

Concerns and actions must be recorded factually, including what was reported, by whom, when, what immediate action was taken and to whom the matter was escalated. Potential evidence should be preserved without unnecessarily viewing, copying or forwarding harmful content. Parents or carers will normally be informed where appropriate unless this could increase risk, compromise an investigation or conflict with safeguarding advice.

The school may refer matters to external agencies, service providers, regulators or the police where required. Serious incidents will be reviewed afterwards so that technical controls, education, procedures or training can be improved.

15. Acceptable Use Agreements and Linked Policies

The school's Acceptable Use Policy and associated agreements form part of the school's online-safety framework and set expectations for the appropriate use of school IT systems, networks and devices by students and staff. Any separate school-managed device or network agreement adopted by the school should be read alongside these arrangements. The Head Teacher is responsible for ensuring that the current Acceptable Use arrangements are identifiable, available and reviewed annually alongside this policy.

Students and staff are expected to comply with the Acceptable Use arrangements applicable to them. Where a separate acknowledgement or agreement is issued, this should be completed at the point determined by the school, normally on joining, when a school-managed device is provided, or following material revision. Parents/carers should be informed of the student expectations and any acknowledgement or consent required.

Linked policies, codes and guidance are: Safeguarding and Child Protection Policy; Behaviour Policy; Privacy & Data Protection Policy; Anti-Bullying Policy; Staff Code of Conduct; Parent/Carer Community Code; and Annex 1 – Qustodio Family Quick Guide.

Operational arrangements for mobile phone confiscation, filtering and monitoring alerts, cybersecurity incidents and lost devices, data breaches, and harmful or sexual imagery are addressed through the school's existing Safeguarding and Child Protection Policy, Behaviour Policy, Acceptable Use arrangements, Privacy & Data Protection Policy and relevant IT processes. These arrangements do not necessarily exist as separate standalone procedures. Staff should follow the relevant policy and established safeguarding, pastoral, IT or data-protection process according to the nature of the incident.

16. Review and Compliance

The Head Teacher will review this policy annually, or sooner following a significant incident, material change in technology, safeguarding guidance or school systems. The review will include input from the IT Team and DSLs and will consider filtering and monitoring arrangements, incident patterns, staff training, Acceptable Use Agreements and the effectiveness of the mobile phone-free procedures.

Failure to comply with this policy may result in action under the Behaviour Policy, Staff Code of Conduct, contractual or disciplinary procedures, safeguarding procedures or other relevant school processes, depending on the person involved and the seriousness of the matter.

Policy Control

Policy Title	E-Safety and Electronic Devices Policy - 2026/2027
Policy Owner	Head Teacher
Responsible Officers	Head Teacher and Senior Leadership Team
Applies to	Whole School Community
Approved by	Executive Director
Date Approved	30 th September 2026
Review Frequency	At least annually and sooner following legal, regulatory, or procedural change
Next Review Date	30 th September 2027
Version	1.0

ANNEX 1 - QUSTODIO FAMILY QUICK GUIDE

Parental controls for students' school-managed devices outside school hours

1. Create your account

Go to **qustodio.com/my-school** and sign up using the personal email address registered with the school. You may be asked for your child's year of birth.

2. Open your child's profile

Select your child from the family dashboard to view activity and configure the available rules.

3. Set parental controls

Choose the controls that suit your family, including **web filtering, blocked apps, content alerts, screen-time, limits and bedtime/routines**.

4. School hours

During school hours, the school manages the school device. **Parent control becomes available when the school day ends.**

5. Additional device

The school provision currently includes protection for the **school laptop outside school hours** and **one additional personal device per student**.

6. Return to Qustodio

After registration, access the parent dashboard at **family.qustodio.com/parents-app**. You do not need to install anything on the student's school-managed device.

Important: Qustodio is provided to support families. Parents and carers remain responsible for supervising and managing their child's use of technology outside school hours.