



LORETO SECONDARY SCHOOL, ST MICHAEL'S
CONVENT ROAD, NAVAN, CO MEATH, C15 YF83

Phone: (046) 902 3830 Email: office@loretonavan.ie Website: www.loretonavan.ie

Acceptable Use Policy

Table of Contents

Defined Terms.....	3
1. Preamble.....	4
2. Purpose of the Policy.....	4
3. Scope of the Policy.....	4
3.1 Linked Policies.....	5
4. Policy Statement and Objectives.....	5
5. Roles and Responsibilities.....	6
5.1 Board of Management (BOM).....	6
5.2 Principal.....	6
5.3 ICT Coordinator.....	6
5.4 Digital Learning Team.....	7
5.5 Staff.....	7
5.6 Students.....	7
5.7 Parents/ Guardians.....	7
5.8 Visitors, Contractors and Other Authorised Users.....	8
6. Acceptable Use Requirements for All Users.....	8
6.1 Responsible and Respectful Use.....	8
6.2 Internet and Online Content.....	8
6.3 Accounts, Passwords and Cybersecurity.....	9
6.4 School and Personal Devices.....	9
6.4.1 Personal Devices.....	10
6.4.2 Assistive Technology.....	10
6.4.3 Removable Storage and Unauthorised Equipment.....	10
6.4.4 Network and System Security.....	10
6.4.5 Authorised Software, Apps and Services.....	11
6.5 Information, Privacy and Data Protection.....	11
6.5.1 Secure Disposal.....	11
6.5.2 Secure Working Practices.....	12
6.6 Email, Messaging and Online Collaboration.....	12
6.6.1 Google Workspace for Education and Google Classroom.....	13
6.6.2 Unique Schools.....	13
6.6.3 VSware.....	13
6.6.4 Athena Tracker.....	14
6.7 Social Media and Online Presence.....	14
6.8 Photography, Video, Audio and Recording.....	15
6.8.1 School Publication and Digital Media.....	16
6.8.2 Podcast Studio and Recording Facilities.....	16
6.9 Copyright, Intellectual Property and Academic Integrity.....	16
6.10 Additional School Guidance.....	17
7. Artificial Intelligence (AI).....	17
7.1 General Requirements.....	17
7.2 Students and the Use of AI.....	17
7.3 Staff and the Use of AI.....	18

8. Additional Requirements for Different Users.....	19
8.1 Staff.....	19
8.1.1 School-Owned ICT Resources.....	19
8.1.2 Working from Home and Remote Access.....	20
8.1.3 Online Meetings and Remote Sessions.....	20
8.1.4 Periods of Absence.....	20
8.1.5 Staff Leaving the School.....	20
8.2 Students.....	20
8.2.1 Student Responsibilities.....	21
8.2.2 Mobile Phones, Smartwatches and Additional Electronic Devices.....	21
8.2.3 Student AUP Guide.....	22
8.3 Parents/ Guardians.....	22
8.4 Visitors, Contractors and Other Authorised Users.....	22
9. Monitoring, Reporting and Breaches.....	23
9.1 Monitoring.....	23
9.2 Reporting Concerns and Incidents.....	23
9.3 Breaches of the Policy.....	24
10. Review of the Policy.....	25
Appendix 1: AI Traffic Light: Guidance for Ethical Use.....	26
Appendix 2: Student AUP Guide.....	27

Defined Terms

This section provides a description of the defined terms used in this Policy. These will be capitalised throughout the document.

Google Classroom	The School's authorised online learning platform used by Staff and Students to support teaching and learning, including the distribution of learning materials, submission of Student work, assignments, class communication and collaboration.
Google Workspace for Education	The School's authorised Google-based digital environment used to support teaching, learning, communication, collaboration and the management and storage of School information.
ICT Resources	Includes computers, laptops, tablets, mobile devices, smart devices, networks, Wi-Fi, internet access, podcasting resources, software, applications, information systems, email, cloud services, digital platforms and other technology provided or authorised by the School.
Parent/ Guardian	A parent or legal guardian of a Student.
School Day	A day on which the school is in operation.
School Systems	The digital systems, applications and platforms provided or authorised by the School for the delivery of educational, administrative, communication or other School-related services, or for the storage, processing or management of School information.
Senior Management	The Principal and Deputy Principals of Loreto Secondary School, St Michael's.
Staff	All employees and other individuals authorised by the School to use School ICT Resources in connection with their duties or responsibilities, including Senior Management, teaching staff, ancillary staff and other authorised personnel.
Student	A student enrolled in Loreto Secondary School, St Michael's.
the School	Refers to Loreto Secondary School, St Michael's.
User	Any person authorised to access or use the School's ICT Resources, including Students, Staff, Parents/ Guardians, Visitors, Contractors and other authorised third parties.

Abbreviated Terms

AI	Artificial Intelligence.
AUP	Acceptable Use Policy.
BOM	Board of Management of Loreto Secondary School, St Michael's.
ICT	Information and Communication Technology.

1. Preamble

Digital technologies are an integral part of modern education and School life. They support teaching, learning, administration and communication and provide Students with opportunities to develop the digital skills, knowledge and understanding needed to use technology safely, responsibly and effectively.

The School provides access to a range of ICT Resources and School Systems, including computers, mobile devices, networks, internet access, software, Google Workspace for Education, Google Classroom, cloud services, information management systems and online communication and collaboration platforms used for School purposes.

Digital technology education forms part of the School's educational provision. Students will have opportunities during their time in the School to develop and apply digital skills and to learn about the safe, responsible, ethical and effective use of digital technologies. This includes developing digital wellbeing and an awareness of the importance of maintaining a healthy and balanced use of technology.

The appropriate use of these technologies is essential to maintaining a secure and effective digital environment. Inappropriate or unsafe use may expose Students, Staff and the wider School community to risks including cyberbullying, inappropriate online behaviour, cybersecurity incidents, loss or unauthorised disclosure of information, malicious software, disruption of School Systems and potential legal or reputational consequences.

This Policy establishes the principles and standards that govern the use of the School's ICT Resources and School Systems. It applies to all Users, while recognising that additional responsibilities may arise from a person's particular role within the School community.

2. Purpose of the Policy

The purpose of this Policy is to establish a clear framework for the safe, responsible, respectful and lawful use of the School's ICT Resources and School Systems.

The Policy aims to:

- support teaching, learning, administration and communication through the effective and responsible use of digital technologies;
- promote digital literacy, responsible digital citizenship and digital wellbeing;
- protect the safety, privacy, dignity and wellbeing of Students, Staff and other members of the School community;
- protect personal, confidential and sensitive information and maintain the security and integrity of the School's ICT Resources and School Systems;
- ensure that Users understand their responsibilities and the requirements that apply to their use of digital technologies, including relevant legislation, regulatory requirements and School policies; and
- provide a clear framework for preventing and addressing inappropriate or unacceptable use.

The School will provide appropriate education, guidance and support to help Users understand and meet their responsibilities under this Policy.

3. Scope of the Policy

This Policy applies to all Users and to the use of the School's ICT Resources, School Systems and digital technologies used for School purposes.

It applies to:

- all ICT Resources provided, owned, leased or otherwise authorised by the School;
- all School Systems and digital technologies used for School purposes;

- the use of School ICT Resources for School-related purposes and, where specifically permitted under this Policy, limited personal use by Staff;
- all connections to the School's network;
- remote access to School Systems;
- personal devices when they are used to access School Systems, School data or School-related services; and
- School-related digital communication and online activity where the provisions of this Policy apply.

The Policy applies whether ICT Resources or School Systems are being used:

- on School premises;
- during School activities, trips or other School-related events;
- while working or learning remotely;
- at home; and
- in any other circumstances where School ICT Resources, School Systems or School-related digital communication are being used.

The general requirements contained in Section 6 apply to all Users.

Sections 7 and 8 set out additional requirements concerning the use of Artificial Intelligence (AI) and for particular groups of Users. These requirements apply in addition to, and do not replace, the general requirements in Section 6.

3.1 Linked Policies

This Policy should be read in conjunction with other relevant School policies and procedures, including, but not limited to:

- Anti-Bullying Policy;
- Bí Cineálta Procedures;
- Child Safeguarding Statement and Child Protection Procedures;
- Code of Behaviour;
- Code of Professional Conduct for Teachers, 2016;
- Complaints Policy and Procedures;
- Data Protection Policy;
- ICT Device Loan Policy; and
- Protected Disclosures Policy.

Where another School policy or procedure specifically addresses a matter, that policy or procedure will also apply.

This Policy will be interpreted and implemented in accordance with applicable legislation and relevant guidance from the Department of Education and other relevant authorities.

4. Policy Statement and Objectives

The School is committed to providing a safe, supportive and effective digital environment in which technology is used appropriately to support teaching, learning, administration and communication.

All Users are expected to consider the potential impact of their actions on the safety, privacy, security, dignity and wellbeing of others, as well as on the integrity and effective operation of the School's ICT Resources and School Systems. Users are also expected to develop and maintain responsible and healthy digital practices that support their own digital wellbeing.

The School will support Users in meeting these responsibilities through appropriate education, guidance, supervision and safeguards. This includes helping Users to develop digital literacy, responsible digital citizenship and healthy digital practices and to understand the safe, ethical and appropriate use of technology.

Where necessary and proportionate, the School may monitor, restrict, suspend or withdraw access to ICT Resources or School Systems in accordance with this Policy, relevant School procedures and applicable legislation.

5. Roles and Responsibilities

The effective implementation of this Policy is a shared responsibility across the School community. While all Users are responsible for complying with this Policy, the nature of those responsibilities will vary according to each person's role within the School.

The responsibilities set out below relate to the implementation of this Policy and should be read together with the general Acceptable Use Requirements in Section 6, the AI requirements in Section 7 and the additional role-specific requirements in Section 8.

5.1 Board of Management (BOM)

The BOM has overall governance responsibility for this Policy.

The BOM will approve the Policy, support its implementation and ensure that appropriate governance arrangements are in place. The BOM will ensure that the Policy is reviewed periodically and updated where necessary to reflect changes in legislation, technology, School practice or identified risks.

5.2 Principal

The Principal has overall responsibility for the implementation and oversight of this Policy within the School.

The Principal will ensure that the Policy is communicated to the School community, that relevant School policies and procedures are followed and that significant concerns or incidents are appropriately managed.

The Principal will ensure that relevant legal, safeguarding, data protection, cybersecurity and School requirements are taken into account in the implementation and review of the Policy.

5.3 ICT Coordinator

The ICT Coordinator has responsibility for coordinating the implementation of this Policy in relation to digital learning and the effective use of ICT Resources and School Systems.

The ICT Coordinator leads the Digital Learning Team and oversees the delivery of Applied Digital Skills lessons, digital learning and related Staff CPD across the School.

The ICT Coordinator provides strategic direction and oversight for the development of digital learning across the School, including appropriate approaches to digital literacy, responsible digital citizenship and digital wellbeing.

The ICT Coordinator is responsible for administering the loan of School-owned ICT Resources to Staff members, including making the ICT Device Loan Policy and Staff ICT Device Loan Agreement Form available and maintaining an up-to-date inventory of the devices allocated to Staff members.

The ICT Coordinator will raise significant concerns relating to digital learning, online safety or the use of ICT Resources and School Systems with the Principal in accordance with relevant School policies and procedures.

5.4 Digital Learning Team

The Digital Learning Team supports the implementation of this Policy through the delivery of digital learning and professional development across the School.

The Digital Learning Team delivers Applied Digital Skills lessons and provides guidance and support to Students in relation to the safe, responsible, ethical and effective use of ICT Resources and School Systems.

The Digital Learning Team supports Staff in developing confidence and competence in the effective and appropriate use of ICT Resources, School Systems and School-authorised digital technologies, including through the delivery of relevant Staff CPD.

The Digital Learning Team supports the implementation of the School's approaches to digital literacy, responsible digital citizenship and digital wellbeing.

Significant concerns relating to digital learning, online safety or the use of ICT Resources and School Systems will be raised with the ICT Coordinator and/or Principal, as appropriate.

5.5 Staff

All Staff are responsible for complying with this Policy and for supporting its effective implementation.

Staff are expected to model responsible and respectful digital behaviour and to support Students in developing safe, responsible and effective digital practices.

Staff must follow relevant School policies, procedures and instructions when using ICT Resources and School Systems and when supporting Students in their use of digital technologies.

Staff must exercise appropriate professional judgement when creating, accessing, recording, storing or sharing School information and must raise safeguarding, data protection, cybersecurity or other significant concerns in accordance with the relevant School policies and procedures.

5.6 Students

Students are responsible for complying with this Policy and the School's Code of Behaviour and for following instructions given by Staff concerning the use of ICT Resources and School Systems.

Students are expected to use technology safely, responsibly and respectfully and to participate appropriately in the School's digital education and guidance.

Students must raise concerns about inappropriate, unsafe or harmful use of technology with a trusted member of Staff.

5.7 Parents/ Guardians

Parents/ Guardians are expected to support the School's approach to the safe, responsible and appropriate use of digital technologies.

They are encouraged to support Students in developing safe and responsible digital habits and in complying with this Policy and the Code of Behaviour.

Parents/ Guardians should use the appropriate School channels to raise concerns relating to the use of ICT Resources, online behaviour or School Systems.

5.8 Visitors, Contractors and Other Authorised Users

Visitors, Contractors and other authorised Users are responsible for complying with this Policy when accessing or using School ICT Resources or School Systems.

They must follow relevant School security arrangements, instructions and procedures and use School ICT Resources only for authorised purposes.

They should raise any suspected security incident, inappropriate use or other concern through the appropriate School channel.

6. Acceptable Use Requirements for All Users

This section applies to all Users of School ICT Resources and School Systems and details the general standards for their safe, responsible, respectful and lawful use, in accordance with this Policy, relevant School policies and procedures, applicable legislation and requirements issued by the School.

6.1 Responsible and Respectful Use

Users must use digital technologies in a way that respects the rights, privacy, dignity and wellbeing of others.

ICT Resources must not be used to harass, intimidate, threaten, bully, impersonate, discriminate against, defame or otherwise harm another person.

Users must not create, access, store, transmit or share material that is illegal, harmful, abusive, threatening, discriminatory, defamatory, hateful, sexually explicit or otherwise inappropriate for the School environment.

Users should consider the potential consequences of digital communication before sending, posting, recording or sharing content. Digital content can be copied, forwarded, reposted or retained beyond the User's control, and Users should therefore exercise appropriate judgement when communicating online.

Online behaviour that constitutes or contributes to bullying behaviour, including cyberbullying, will be addressed in accordance with the School's Bí Cineálta Procedures, Code of Behaviour and other relevant policies.

Where appropriate, the School may address online behaviour occurring outside School where it has a clear and significant impact on Students, Staff, other members of the School community or the operation of the School.

6.2 Internet and Online Content

Users must use School internet access and online services appropriately and comply with applicable restrictions, filtering and access controls implemented by the School.

Users must not intentionally access, download, upload, transmit, store or distribute material that is unlawful, harmful or inappropriate. This includes child sexual abuse material, serious violence, unlawful discrimination, hatred, exploitation or other content that would be inappropriate or harmful in the context of School use.

Users must not use ICT Resources to unlawfully download, upload or distribute material, including through unauthorised file sharing, torrenting or other peer-to-peer services.

Users must not engage in unnecessary or excessive activity that places unreasonable demands on the School network or adversely affects access to services by other Users.

Users must not attempt to bypass, disable or circumvent content filtering, network restrictions, security controls or other technical safeguards implemented by the School. This includes using unauthorised proxy services, virtual private networks (VPNs), software, devices or other methods to circumvent School restrictions or security controls.

ICT Resources must not be used to conduct private commercial activities, operate a personal business or generate personal financial gain unless specifically authorised by the School.

6.3 Accounts, Passwords and Cybersecurity

Users are responsible for protecting the security of their own accounts and access credentials and for taking appropriate steps to prevent unauthorised access.

Passwords, authentication codes and other credentials must be kept confidential and must not be shared with another person.

Users must not approve authentication requests or provide authentication codes where they did not initiate or expect the request.

Users must not pressure, threaten, coerce or otherwise attempt to force another User to disclose their password or other credentials.

Users must remain alert to phishing, fraudulent messages, suspicious links, unusual requests for information and other potential security threats.

Users must not attempt to access another person's account, files, communications or information without appropriate authorisation.

Users must not create, install or distribute malicious software, viruses, code or other material designed or intended to damage, disrupt or compromise School ICT Resources or School Systems.

Users must not undertake network scanning, vulnerability testing, penetration testing or similar security activity unless explicitly authorised by the School.

Suspected phishing, unauthorised access, loss of credentials or other cybersecurity incidents must be reported promptly to the ICT Coordinator, a Deputy Principal or the Principal.

6.4 School and Personal Devices

ICT Resources remain the property of the School unless otherwise specified.

Users are responsible for taking care of ICT Resources made available to them and for using such equipment only for authorised purposes.

Users must take precautions to protect ICT Resources from loss, theft, damage, misuse and unauthorised access. School devices must not be left unattended where they may be lost, stolen or accessed by an unauthorised person.

Users must not modify, reconfigure, repair or otherwise interfere with ICT Resources, whether themselves or through a third party, unless authorised to do so.

ICT Resources must not be removed from the School, lent or made available to another person, or used for purposes outside the User's authority without appropriate permission.

6.4.1 Personal Devices

Personal devices must only be used to access School Systems or School information where such use is authorised by the School.

Where a personal device is authorised for School-related purposes, the User must take appropriate steps to protect the device, their account and any School information accessed through it. This includes keeping the device and relevant software up to date, using appropriate security measures such as a passcode or other device lock and taking care to prevent unauthorised access to School information.

School information must not be transferred to, stored on or accessed through personal devices or personal storage services unless this has been authorised by the School and is consistent with the School's data protection and security requirements.

Users must comply with the requirements of this Policy and the School's Code of Behaviour concerning the use of personal devices, including mobile phones, smartwatches and recording devices.

6.4.2 Assistive Technology

The School recognises that assistive technology can support Students with accessibility, communication, learning, medical or other identified needs.

Assistive technology may be used where it has been authorised by the School and where its use supports the Student's identified needs or educational participation. The School will take appropriate account of a Student's individual needs when applying this Policy and may make reasonable arrangements to facilitate the appropriate use of assistive technology.

Where assistive technology involves the use of a personal device, the Student must use the device in accordance with the arrangements or instructions provided by the School and only for the authorised purpose.

The use of assistive technology must not compromise the privacy, safety, security or learning environment of other Students or Staff. Where a device or technology has functionality beyond its authorised purpose, including recording, photography, communication or internet access, those functions must only be used where specifically authorised by the School.

Any information accessed, created, stored or communicated through assistive technology in connection with School activities must be handled in accordance with this Policy, the School's Data Protection Policy and other relevant School policies and procedures.

6.4.3 Removable Storage and Unauthorised Equipment

Users must not connect unauthorised peripheral devices, equipment or removable storage to School ICT Resources or the School network.

Where removable storage is permitted, Users must comply with any School requirements concerning its use and security.

Users must not use removable storage or other equipment to introduce unauthorised software, malware or other material that may compromise ICT Resources and School Systems.

6.4.4 Network and System Security

Users must not attempt to gain unauthorised access to School networks or School Systems, or deliberately interfere with or disrupt network or system services.

Users must not use personal devices, software, applications or other equipment to circumvent School restrictions or security controls.

Users must not alter, disable or interfere with the technical configuration or security settings of ICT Resources or School Systems unless authorised to do so.

6.4.5 Authorised Software, Apps and Services

Users must not install, download or use software, applications, browser extensions or other digital services on School devices or School Systems unless authorised by the School.

Staff must not introduce or use software, applications or online services for School purposes without prior authorisation from the School. Requests to introduce or use such software, applications or online services must be referred to the ICT Coordinator and/or the Principal for consideration.

Users must not disable, bypass or interfere with security controls or other technical restrictions applied to ICT Resources or School Systems.

6.5 Information, Privacy and Data Protection

Users must respect the privacy and confidentiality of information accessed through ICT Resources and School Systems.

Personal, confidential or otherwise sensitive information must only be accessed, used, stored, shared or disclosed for a legitimate and authorised purpose.

Users must only access information they are authorised to access and must take steps to prevent unauthorised persons from accessing School information, including when working remotely or when using shared or personal devices.

School information, particularly personal, confidential or sensitive information, must be stored only using School Systems, unless otherwise authorised by the School. Users must not store such information on personal storage devices, personal cloud services or unauthorised applications or platforms.

Users must comply with the School's Data Protection Policy and relevant procedures concerning the collection, use, storage, sharing, security and retention of personal data.

School Systems and digital technologies used for School purposes may be used to collect, store and process information relating to Students, Staff and School activities for legitimate School purposes. Users must only access and use such information in accordance with their authorised role, the purpose for which the information is held and any relevant School requirements.

6.5.1 Secure Disposal

School information must be handled, retained, deleted and securely disposed of in accordance with the School's Data Protection Policy, applicable legal requirements and relevant School procedures. Storage media containing School information must be securely handled, transferred, erased or disposed of as appropriate.

Users must not dispose of, reassign, hand over, transfer custody of, repurpose, alter or otherwise relinquish control of ICT Resources unless authorised by the School and in accordance with relevant School procedures.

Users must not remove, disable, interfere with or bypass security controls or other safeguards applied to ICT Resources or School Systems, including measures used to securely remove School information.

Where School information is stored on removable, portable or other storage media, Users must follow relevant School procedures to ensure that the information is securely transferred to an authorised School System before the media is disposed of, repurposed or returned, where applicable.

6.5.2 Secure Working Practices

Users accessing confidential, personal or sensitive School information must take appropriate steps to prevent that information from being viewed, accessed or disclosed by or to unauthorised persons.

Users must take reasonable steps to ensure that personal, confidential or sensitive School information is not inadvertently displayed on screens, projectors, interactive displays or other shared displays.

Users must lock their screens or otherwise secure ICT Resources when leaving them unattended.

Users should not leave confidential, personal or sensitive School information unattended or visible in printed or physical form and should securely store such information when leaving their workspace.

Staff must take particular care when working in shared or public spaces to prevent unauthorised persons from viewing or accessing School information.

Where confidential, personal or sensitive information is printed, scanned or copied, Users should collect it promptly from the relevant device and take appropriate steps to prevent unauthorised access.

6.6 Email, Messaging and Online Collaboration

School email accounts, messaging services and online collaboration and communication platforms used for School purposes must be used appropriately and primarily for legitimate School-related purposes.

Staff and Students must use School-provided or School-authorised email accounts and communication platforms for School-related communication and must not use personal email accounts or personal messaging services for School-related communication unless specifically authorised by the School.

Users must communicate in a respectful, appropriate and professional manner. Messages, files, links, images and other material shared through School Systems must be lawful, appropriate and relevant to the purpose for which the service is being used.

Users must not use School communication systems to send unsolicited bulk messages, spam or other inappropriate mass communications.

Users must exercise particular care when communicating with Students, Staff, Parents/ Guardians and external persons. Professional boundaries must be maintained at all times, and communication must comply with relevant School policies, procedures and professional requirements.

School-related communication should, where reasonably practicable, take place during normal School or working hours. Staff should not ordinarily be expected to respond to School-related communications outside their normal hours of work. This does not prevent communication outside these hours where there is a legitimate operational, educational, safeguarding or emergency need.

Users must not use School communication systems to harass, threaten, intimidate, impersonate or otherwise harm another person.

Users must exercise caution when opening attachments, clicking links or responding to requests for passwords, authentication codes, financial information or other sensitive information. Where there is any doubt about the legitimacy of a message or request, Users must not respond, click on links or open

attachments and must report the concern promptly to the ICT Coordinator, a Deputy Principal or the Principal, as appropriate.

6.6.1 Google Workspace for Education and Google Classroom

The School uses Google Workspace for Education and Google Classroom as School Systems to support teaching, learning, communication and collaboration.

Staff and Students must use their School-authorised Google accounts when accessing Google Workspace for Education and Google Classroom for School-related purposes.

Google Classroom is used to support teaching and learning, including the sharing of learning materials, communication relating to classes, distribution and submission of assignments and Student work, and other School-related learning activities.

Users must use Google Workspace for Education and Google Classroom appropriately, responsibly and respectfully and in accordance with this Policy, the School's Data Protection Policy, safeguarding requirements and instructions issued by the School.

Users must not share their School Google account passwords or allow another person to access their account. Users must only access Google Classroom classes, files, documents and other information for which they have been authorised.

School information must not be transferred to or shared through personal Google accounts or other unauthorised platforms or services unless specifically authorised by the School.

Staff must exercise appropriate professional judgement when creating, sharing, storing or communicating School information through Google Workspace for Education and Google Classroom, particularly where Student personal, confidential or sensitive information is involved.

6.6.2 Unique Schools

The School uses Unique Schools as a School System for communication, administration and the management of information relating to Students, Parents/ Guardians and School activities.

Unique Schools is used for School communications, attendance and related notifications, digital forms and permissions, access to relevant Student information, School-related payments and other School-related administrative and communication purposes.

Parents/ Guardians must use Unique Schools appropriately for School-related purposes and must keep their account details and access credentials secure.

Information accessed or obtained through Unique Schools must be handled in accordance with the School's Data Protection Policy and must not be shared or disclosed to unauthorised persons or transferred to unauthorised applications, platforms or services.

Users must follow relevant directions and requirements issued by the School concerning the use of Unique Schools.

6.6.3 VSware

The School uses VSware as the School's Management Information System (MIS) for the administration and management of information relating to Students and the operation of the School.

VSware supports School functions including attendance, timetabling, assessment and reporting, behaviour and Student tracking, administration and communication with Parents/ Guardians.

Authorised Staff may use VSware to record and access information necessary for their School duties. Information recorded must be appropriate, accurate and relevant to the purpose for which it is recorded. Staff must exercise appropriate professional judgement when recording information about Students.

Access to VSware is controlled according to the User's role and level of authorisation. Users must only access information and functions necessary for their legitimate School purposes and must keep their account details and access credentials secure.

Parents/ Guardians may be provided with access to information relating to their child through an authorised VSware account. They must use their own account and must not attempt to access information relating to another Student or information or functions that are not available to them.

Students may be provided with access to information relating to themselves in accordance with the School's procedures and applicable data protection requirements.

Information accessed or obtained through VSware must be handled in accordance with the School's Data Protection Policy and must not be shared or disclosed to unauthorised persons or transferred to unauthorised applications, platforms or services.

6.6.4 Athena Tracker

The School uses the Athena Tracker as a School System to support the monitoring of Student academic progress, the identification of intervention needs and the provision of appropriate Student support.

Access to the Athena Tracker is restricted to authorised Staff. The Athena Tracker may only be used for legitimate School purposes connected with teaching, learning, Student support and academic monitoring.

Users must only use their own authorised Athena Tracker account and must keep their account details, passwords and other access credentials secure and confidential. Users must not share their credentials or allow another person to access the Athena Tracker using their account.

Information entered or updated in the Athena Tracker must be accurate, appropriate and relevant to the purpose for which it is recorded. Teachers must take reasonable care when entering or updating Student information and must report any suspected errors, discrepancies or inaccuracies to the Academic Tracking Coordinator, and any technical or access-related issues to the ICT Coordinator.

Information accessed through the Athena Tracker must be treated as confidential and handled in accordance with the School's Data Protection Policy and applicable data protection requirements. Student information must only be accessed, used or shared where there is a legitimate and authorised School purpose, and must not be disclosed to unauthorised persons or transferred to unauthorised applications, platforms or services.

Information and analytics provided through the Athena Tracker must be used only to support Student academic progress, identify appropriate intervention or support needs and facilitate informed and appropriate discussions with Students and Parents/ Guardians. The Athena Tracker must not be used for personal, commercial or other non-educational purposes.

6.7 Social Media and Online Presence

The School recognises that social media and other online platforms can provide opportunities for communication, learning, collaboration and engagement. Users are nevertheless expected to exercise appropriate judgement and behave responsibly when using such services.

Users must not use social media or other online platforms to harass, bully, threaten, intimidate, impersonate, defame or otherwise harm another member of the School community. This includes creating, sharing, forwarding or engaging with content where such activity contributes to harm.

Users must respect the privacy and confidentiality of Students, Staff and other members of the School community and must not share personal, confidential or sensitive information, including images or recordings, without appropriate authority or consent.

Users must not create or use fake accounts or profiles to impersonate another person or the School.

Users must not create, generate, manipulate, alter, share or distribute deepfakes, fake or misleading images, videos, audio recordings or other digital content, including content generated or altered using artificial intelligence (AI) or other technologies, where the purpose or reasonably foreseeable effect is to impersonate, harass, threaten, defame or otherwise cause harm to a Student, Staff member, the School or another member of the School community. Users must not present fabricated or manipulated content as genuine where doing so could cause harm, materially misrepresent a person or event, or falsely imply that the School or a member of the School community has said or done something.

Users must not represent personal views as those of the School or imply that they are speaking on behalf of the School unless authorised to do so. The School's name, logo, branding or other identifying material must not be used on personal accounts or platforms in a way that implies that the account or content is an official School account or communication, or that the School has endorsed the content, without appropriate authorisation.

School-related concerns or complaints should be raised through the appropriate School procedures rather than through public social media or other online forums. Parents/ Guardians and Students aged 18 or over should use the School's Complaints Policy and Procedures where applicable. Public discussion of School-related concerns should be avoided where it could compromise the privacy or dignity of those involved.

Staff must also comply with the Code of Professional Conduct for Teachers, 2016, where applicable, and maintain appropriate professional boundaries when using social media or communicating electronically.

The School may address online behaviour occurring inside or outside School where it has a clear and significant impact on Students, Staff, other members of the School community or the operation or reputation of the School. Any such concerns will be addressed in accordance with the relevant School policies and procedures, including the Code of Behaviour and Bí Cineálta Procedures.

6.8 Photography, Video, Audio and Recording

The taking, use, storage and publication of photographs, video and audio recordings must comply with the School's consent, safeguarding and data protection requirements.

Users must not photograph, record or otherwise capture, create or generate an image, voice recording or other identifiable representation of another person without appropriate permission or authorisation.

Users must not use, share, create, publish or distribute photographs, video or audio recordings of Students, Staff or other members of the School community without appropriate permission or authorisation.

Recordings must not be created, shared or used for the purpose of humiliating, embarrassing, bullying, threatening or otherwise harming another person.

The creation, possession, sharing or distribution of intimate, sexualised or otherwise inappropriate images or recordings involving Students or other minors is strictly prohibited and may constitute a serious safeguarding or criminal matter.

6.8.1 School Publication and Digital Media

Photographs, video, audio recordings or examples of Student work intended for publication on the School website, official social media accounts, podcasts or other public-facing platforms must be authorised by the School and comply with applicable consent, safeguarding and data protection requirements.

Student work or other material created for School purposes must not be published on personal websites, social media accounts or other external platforms without appropriate permission.

6.8.2 Podcast Studio and Recording Facilities

The School's podcast studio, recording equipment and associated technologies are ICT Resources and must be used only for authorised educational, curricular, extracurricular or other School-related purposes.

Users must follow instructions concerning the use of the facilities and take appropriate care of recording equipment and associated technology.

Users must not alter, remove or install equipment or software without authorisation.

Recording, creating or publishing the voice, image, name or other identifiable information of Students, Staff or other individuals through School recording facilities must only take place for an appropriate School purpose and in accordance with the School's applicable consent and permission requirements. This includes obtaining the required consent from podcast guests and, where applicable, the required Parent/ Guardian permission for Student participation.

Recordings created using School facilities or equipment must be stored, edited and shared using School Systems and other authorised services. School-related recordings and digital media must not be uploaded to external platforms unless the platform has been authorised by the School for the intended purpose and the necessary permissions and safeguards are in place.

6.9 Copyright, Intellectual Property and Academic Integrity

Users must respect copyright, licensing, intellectual property and other rights relating to digital content.

Users must not copy, download, reproduce, distribute or use copyrighted material in a way that infringes copyright or licensing requirements. Where material created by another person is used, appropriate acknowledgement or attribution should be provided.

Students must comply with School requirements relating to plagiarism, academic integrity and the appropriate acknowledgement of sources. Any additional requirements issued by the School or the State Examinations Commission in relation to assessed work or examinations must also be followed.

Students must not submit work created wholly or substantially by another person as their own or misrepresent the source or authorship of work submitted for assessment.

The use of AI and other digital tools in learning and assessment must comply with the requirements set out in Section 7 of this Policy.

Users retain intellectual property rights in their own original work, subject to applicable law, agreements and School policies.

6.10 Additional School Guidance

The School may issue additional guidance, requirements or instructions concerning the use of ICT Resources, School Systems and digital technologies for School purposes. Users must comply with such guidance, requirements and instructions.

Such guidance must be consistent with this Policy, relevant School policies and procedures, and applicable legislation. Where a matter requires a change to this Policy, the Policy will be reviewed and updated in accordance with Section 10.

7. Artificial Intelligence (AI)

The School recognises that AI can provide valuable opportunities for teaching, learning, administration and creative work. AI tools must nevertheless be used responsibly, ethically and in accordance with this Policy, relevant School requirements and other relevant School policies.

7.1 General Requirements

All Users must use AI responsibly and must consider the potential impact of their use on others.

AI must not be used to create, generate or distribute content that is offensive, harmful, discriminatory, threatening, misleading or otherwise inappropriate. Users must respect the privacy, rights and intellectual property of others and must not use AI in a manner that could result in harmful, dangerous or unlawful outcomes.

Users must not enter personal, confidential, sensitive or otherwise protected School information into an AI system unless the use of that system has been specifically authorised and appropriate safeguards are in place.

AI-generated material must be treated critically and, where appropriate, checked for accuracy, reliability, bias and suitability before being relied upon or shared. Users should be aware that AI systems may produce inaccurate, misleading or fabricated information.

7.2 Students and the Use of AI

Students must comply with the School's requirements concerning the use of AI in homework, assignments, projects, examinations and other assessed work. The instructions given by a teacher for a particular task will determine whether and how AI may be used, where relevant.

Where AI use is permitted, it should support the Student's own learning, thinking and creativity rather than replace them. Students remain responsible for the work they submit and must be able to demonstrate their own knowledge, skills and understanding.

Students must not use AI to:

- complete work that they are required to complete themselves;
- present AI-generated or AI-assisted work as entirely their own where such use has not been permitted or acknowledged as required;
- misrepresent their knowledge, skills, understanding or achievement;
- generate inappropriate, harmful or offensive content;
- harass, bully, threaten or otherwise harm another person; and
- breach this Policy or other applicable School policies or procedures.

Students must clearly acknowledge and document their use of AI in assessed or submitted work where required by the School, a teacher or the relevant assessment or examination authority. For State Examination coursework and other externally assessed work, Students must also comply with any additional requirements concerning the use and acknowledgement of AI set by the relevant examination authority and the School.

Students should use the AI Traffic Light Guidance (see Appendix 1) when considering whether and how AI may appropriately be used in their schoolwork. The guidance provides a simple framework for distinguishing between uses of AI that may be appropriate, uses that require consultation with a teacher and uses that are not permitted. Teacher instructions for a particular task take precedence over the general guidance.

Where a Staff member has a reasonable concern about the authenticity or authorship of a Student's work, including concerns regarding unauthorised or inappropriate use of AI, the Staff member may seek further information or clarification from the Student and/ or request evidence of the Student's learning process, knowledge, skills or understanding. Where the authenticity of the work cannot be established in accordance with the requirements of the relevant assessment or examination authority, the matter will be referred and dealt with in accordance with the applicable assessment, School and State Examinations Commission procedures.

7.3 Staff and the Use of AI

Staff may use AI to support teaching, learning, administration and communication where such use is appropriate, responsible and consistent with this Policy and relevant School requirements.

Before using an AI tool, Staff must consider, as appropriate:

- data protection and confidentiality;
- safeguarding and Student welfare;
- accuracy, reliability and potential bias;
- intellectual property and copyright;
- the suitability and appropriateness of AI-generated content;
- the age, needs and circumstances of Students who may encounter or be affected by AI-generated content;
- the potential for over-reliance on AI; and
- their professional responsibilities and the need to exercise appropriate professional judgement.

AI should support, and not replace, professional judgement and human decision-making. Staff remain responsible for reviewing and verifying AI-generated material before relying upon it, sharing it with Students, colleagues, Parents/ Guardians or other parties, or using it in School communications, teaching materials, administrative work or decision-making.

Staff must not enter personal, confidential, sensitive or otherwise protected information relating to Students, Parents/ Guardians, Staff or the School into an AI system unless the use of that system has been specifically authorised and appropriate safeguards are in place.

Any use of AI by Staff must comply with this Policy and with relevant School policies and procedures, including those relating to data protection, safeguarding, acceptable behaviour, confidentiality and professional conduct.

When Students complete assessments for the State Examinations Commission, Staff will use appropriate professional judgement when considering the authenticity and authorship of Student work, having regard to relevant evidence of the Student's learning, development, knowledge, skills and understanding. Where appropriate and in accordance with School procedures, Staff may also consider information provided by AI detection tools or other technological indicators. Such tools will not, in isolation, be regarded as establishing that AI has been used or that academic misconduct has occurred.

Where a serious concern arises regarding the authenticity or authorship of Student work for a State Examinations Commission assessment, the Staff member should record the concern and relevant evidence and refer the matter to the Senior Cycle Redevelopment (SCR) Co-ordinator, who will liaise with the Principal as appropriate. The matter will then be dealt with in accordance with the relevant assessment requirements, School procedures and State Examinations Commission procedures.

8. Additional Requirements for Different Users

This section sets out additional requirements and responsibilities that apply according to a User's role within the School community. These requirements apply in addition to, and do not replace, the general requirements in Sections 6 and 7.

8.1 Staff

Staff have additional responsibilities arising from their professional role and their access to School Systems, School information and Students.

Staff must use ICT Resources in a manner consistent with their professional responsibilities and the Code of Professional Conduct for Teachers, 2016. Staff are expected to model responsible and respectful digital behaviour and to maintain appropriate professional boundaries when communicating with Students, Parents/Guardians and other members of the School community.

Staff must take particular care when accessing or processing Student, Staff or other personal information and must comply with applicable data protection, safeguarding, confidentiality and professional requirements.

Staff must use Google Workspace for Education and Google Classroom through their School-authorised accounts for School-related teaching, learning and communication. Staff must use Google Classroom in accordance with this Policy, the School's Data Protection Policy, safeguarding requirements and professional responsibilities.

When using Google Classroom, Staff must take appropriate care when creating, sharing, storing or communicating Student information and must ensure that information is shared only with Students or other authorised Users who require access for legitimate School purposes. Staff must maintain appropriate professional boundaries in all online communication with Students.

Online collaboration and communication platforms provided or designated by the School must be used for School-related communication with Students, particularly where an appropriate School channel is available. Staff must not use personal messaging services for routine School communication with Students where an appropriate School-authorised alternative is available.

Staff must exercise appropriate judgement when using social media and other public-facing platforms and must comply with the requirements set out in Section 6.7 of this Policy. Staff must not present personal opinions as official School views or imply that they are speaking on behalf of the School unless authorised to do so.

Staff must follow applicable School procedures when responding to safeguarding, data protection, cybersecurity or other significant concerns arising from their use of ICT Resources.

When using projectors, interactive displays or other shared classroom displays, Staff must take reasonable steps to prevent School information from being inadvertently disclosed. Staff should close or minimise applications containing personal, confidential or sensitive information and disconnect from or stop displaying their device when leaving the classroom, where appropriate.

Limited personal use of School ICT Resources by Staff may be permitted, provided that such use is reasonable, does not interfere with School activities or the Staff member's responsibilities, does not create unreasonable cost or risk for the School, and complies with this Policy and other relevant School policies.

8.1.1 School-Owned ICT Resources

Where a School ICT Resource is loaned to a Staff member, the Staff member must comply with the School's ICT Device Loan Policy and complete the Staff ICT Device Loan Agreement Form at the time of the loan.

The signed agreement sets out the Staff member's responsibilities in relation to the use, care, security and return of the equipment. The ICT Device Loan Policy and Staff ICT Device Loan Agreement Form are available from the ICT Coordinator.

8.1.2 Working from Home and Remote Access

Where Staff are authorised to work from home or access School Systems remotely, they must:

- use School ICT Resources and School Systems;
- take appropriate steps to prevent unauthorised access to School Systems, accounts and information;
- ensure that School information is not accessible to other household members or visitors; and
- comply with this Policy and the School's Data Protection Policy when working remotely.

8.1.3 Online Meetings and Remote Sessions

Staff conducting or attending online meetings or remote sessions for School purposes must:

- use School platforms and accounts;
- take appropriate steps to ensure that meetings, conversations and shared information cannot be accessed, viewed or overheard by unauthorised persons;
- protect Student, Staff and other personal, sensitive or confidential information shared during the meeting or session;
- not record meetings or sessions unless the recording is authorised and the necessary consent, safeguarding, data protection and security requirements are satisfied; and
- store any School information, notes, recordings or other records arising from the meeting or session using School Systems.

Where Staff conduct or attend live online teaching sessions, they must take particular care when sharing screens, documents or other content to ensure that personal, sensitive or confidential information is not inadvertently disclosed. Live teaching sessions must only be recorded where authorised and in accordance with the School's consent, safeguarding, data protection and security requirements.

8.1.4 Periods of Absence

Where Staff are absent from the School for an extended or planned period, they must, where appropriate, ensure that School information, files, records and communications necessary for the continuation of School business are stored using School Systems and can be accessed by authorised colleagues in accordance with the School's procedures and data protection requirements.

8.1.5 Staff Leaving the School

When a Staff member leaves the School, they must return any School-owned ICT Resources and other School property provided to them.

Staff must not retain, copy or transfer School information, files or data after their employment or authorised access ends, except where authorised by the School.

The School may restrict, suspend or withdraw access to School Systems, accounts and ICT Resources when a Staff member leaves the School or no longer requires access.

8.2 Students

This section sets out additional requirements and responsibilities that apply to Students when using ICT Resources, School Systems and digital technologies. These requirements should be read together with the general requirements in Section 6 and the Artificial Intelligence requirements in Section 7.

8.2.1 Student Responsibilities

Students are expected to use ICT Resources in accordance with this Policy, the Code of Behaviour and instructions given by Staff.

Students must use technology responsibly and respectfully, protect their accounts and passwords, respect the privacy and dignity of others and use School Systems and digital technologies only for authorised purposes.

Students must not use technology to bully, harass, threaten, impersonate or deliberately embarrass another person. Students must not photograph, record or distribute images, video or audio of other Students, Staff or members of the School community without appropriate permission or authorisation.

Students must use Google Workspace for Education and Google Classroom in accordance with this Policy and their teachers' instructions. Students must use Google Classroom for authorised educational purposes and must not access, alter, delete, share or interfere with another Student's work, files, account or class materials. Students must not use Google Classroom to post, upload or share content that is inappropriate, harmful, offensive or unrelated to the intended educational purpose.

Students must follow School requirements concerning the use of personal devices, mobile phones, recording equipment and other technology during the School Day, School activities and School events.

Students must raise concerns about inappropriate, unsafe or harmful online activity with a trusted member of Staff.

Students must not arrange to meet in person with someone they have only come to know through the internet or other online communication without the knowledge and involvement of a Parent/ Guardian and, where relevant, appropriate advice or support from the School.

8.2.2 Mobile Phones, Smartwatches and Additional Electronic Devices

Students must comply with the School's requirements concerning mobile phones, smartwatches, listening devices such as headphones, gaming devices and other personal electronic devices.

Mobile phones must be switched off and kept securely in the Student's assigned locker as required by the School during the School Day and must not be used unless specifically authorised.

Students must not use mobile phones, smartwatches, headphones or other personal electronic devices during the School Day except where their use has been specifically authorised for educational, medical, accessibility, assistive technology or safeguarding purposes.

Students must not use personal devices to photograph, record, livestream or otherwise capture Students, Staff or other persons without appropriate permission or authorisation.

Students must not use personal devices to access, record, store or distribute School information unless specifically authorised.

Gaming devices and other electronic devices must not be used during the School Day unless specifically authorised by the School.

Where a Student needs to contact a Parent/ Guardian during the School Day, the Student must do so through the School Office or in accordance with the School's designated arrangements, rather than using a personal device, unless otherwise authorised.

Students must comply with instructions from Staff concerning the storage, use or removal of personal electronic devices.

During State Examinations and other formal assessments, Students must comply with any additional requirements issued by the School and the relevant examination authority concerning mobile phones, smart devices and other electronic devices.

8.2.3 Student AUP Guide

The School provides student-friendly visual guidance to help Students understand and remember the key expectations set out in this Policy. The Student AUP Guide (Appendix 2) provides a visual summary of the School's expectations for the safe, responsible and respectful use of technology.

The Student AUP Guide is intended to support Students' understanding of this Policy and does not replace or alter its requirements.

8.3 Parents/ Guardians

This section sets out additional expectations that apply to Parents/ Guardians in supporting the School's approach to ICT use.

Parents/ Guardians should encourage Students to develop safe and responsible digital habits and should support them in complying with this Policy and the Code of Behaviour.

Parents/ Guardians are required to complete the Parent/ Guardian Consent Form for Google Workspace for Education and Third-Party Apps. The School will provide this form to Parents/ Guardians for completion. The form is normally provided when a Student enters First Year or, in the case of a Student under 18 enrolling during the school year, at the time of enrolment. The completed form remains applicable for the duration of the Student's enrolment in the School. Parents/ Guardians who wish to review the form or seek clarification about the consent provided may contact the School Office.

Parents/ Guardians should communicate appropriately and respectfully with the School and should respect the privacy, dignity and rights of Students, Staff and other members of the School community.

Concerns relating to the use of ICT Resources, online behaviour or the operation of School Systems should be raised through the appropriate School channels rather than through inappropriate online or social media activity.

Parents/ Guardians must not publish or share photographs, video, audio recordings or personal information relating to Students, Staff or School activities where doing so could compromise privacy, safeguarding or the rights of others.

Where Parents/ Guardians are provided with access to School Systems, they must use their own authorised accounts, protect their access credentials and only access information and functions available to them.

8.4 Visitors, Contractors and Other Authorised Users

Visitors, Contractors and other authorised Users must use ICT Resources only for authorised purposes, must only access School Systems and information necessary for their authorised role and must comply with relevant School security arrangements and instructions.

They must protect the confidentiality and security of School information and must not access, copy, disclose or retain information beyond what is necessary for their authorised role.

Visitors, Contractors and other authorised Users must promptly report any suspected security incident, data breach, inappropriate use, loss of equipment or other concern arising from their use of ICT Resources to the

ICT Coordinator, a Deputy Principal or the Principal, as appropriate, and follow any relevant School procedures.

9. Monitoring, Reporting and Breaches

The School has a responsibility to protect Students, Staff and other Users, School information and ICT Resources. Appropriate monitoring and reporting arrangements support the safe and secure use of technology within the School.

The School will balance the need for security and accountability with the privacy and rights of Users.

Monitoring, reporting and any action arising from concerns or suspected breaches will be carried out in accordance with this Policy, relevant School policies and procedures and applicable legislation.

9.1 Monitoring

The School may monitor and record the use of its ICT Resources and School Systems where necessary for a legitimate School purpose and in accordance with applicable law, data protection requirements and relevant School policies and procedures.

Monitoring may be carried out for purposes including:

- maintaining the security and operation of networks and School Systems;
- detecting and responding to security incidents, unauthorised access or inappropriate use;
- investigating actual or suspected breaches of this Policy or other School policies and procedures;
- protecting School information, ICT Resources and the School community;
- investigating technical faults and maintaining School Systems performance;
- supporting safeguarding and the protection of Students and other Users;
- complying with legal or regulatory obligations; and
- investigating suspected unlawful activity.

Monitoring may involve automated systems, system logs, security tools, content-filtering systems and other technical measures. It may also involve authorised Staff accessing relevant information where necessary for a legitimate School purpose.

The School does not monitor individual Users solely for the purpose of observing their activities without a legitimate School purpose. Monitoring will be carried out in accordance with the principles of necessity and proportionality and applicable data protection requirements.

Information obtained through monitoring will only be accessed and used for legitimate purposes and retained only for as long as necessary and in accordance with applicable retention requirements.

Users should be aware that information processed using ICT Resources or School Systems may be accessed by authorised Staff where necessary for a legitimate School purpose and in accordance with applicable requirements.

School-managed accounts and School Systems may use automated security, safety, monitoring or content-filtering measures. Where such measures generate an alert or concern, authorised Staff may review relevant information where necessary for a legitimate School purpose and in accordance with the School's Data Protection Policy and applicable requirements.

9.2 Reporting Concerns and Incidents

All Users have a responsibility to raise concerns about the inappropriate, unsafe or unauthorised use of ICT Resources or School Systems.

Examples of concerns that should be reported include:

- cyberbullying or inappropriate online behaviour;
- suspected unauthorised access to accounts or School Systems;
- loss, theft or damage of School devices or equipment;
- data breaches or unauthorised disclosure of information;
- phishing, malware or other security threats;
- inappropriate or unlawful content;
- unauthorised recording or sharing of photographs, video or audio;
- misuse of School Systems, accounts or devices; or
- any other suspected breach of this Policy.

Concerns should be reported promptly to an appropriate member of Staff. Concerns involving phishing, unauthorised access, compromised accounts or loss of credentials should be reported to the ICT Coordinator, a Deputy Principal or the Principal. Students may also raise concerns about inappropriate, unsafe or harmful online activity with a trusted member of Staff.

Where inappropriate or potentially harmful material is accidentally accessed, Users should not continue to view, copy, save, download or distribute the material. The matter should be reported promptly to an appropriate member of Staff.

Users should not attempt to investigate, confront or resolve serious incidents themselves where doing so could increase risk, compromise evidence or interfere with an appropriate School response.

Where a concern involves safeguarding, data protection or another matter requiring specialist action, the School will respond in accordance with the applicable School policy or procedure.

9.3 Breaches of the Policy

The School expects all Users to comply with this Policy. Breaches may range from inadvertent or minor incidents to serious or deliberate misuse.

Where a concern or suspected breach arises, the School will respond in a manner that is proportionate to the circumstances.

In deciding how to respond, the School may consider:

- the nature and seriousness of the conduct;
- whether the breach was deliberate, reckless or accidental;
- the impact on Students, Staff, other Users or the School;
- whether personal, confidential or sensitive information was involved;
- whether School Systems, devices, networks or security were compromised;
- whether there is evidence of repeated or persistent inappropriate use;
- whether the User has previously been advised or instructed about the relevant requirement; and
- whether the conduct may constitute an offence or other legal or regulatory breach.

A breach of this Policy may result in action under the applicable School policy or procedure.

Student breaches will normally be addressed under the Code of Behaviour and, where applicable, other School policies or procedures.

Staff breaches may be addressed in accordance with the applicable disciplinary procedures for teachers and principals and, where applicable, other School policies or procedures.

Concerns regarding the conduct of Parents/ Guardians may be addressed under the School's applicable communication, complaints or other procedures.

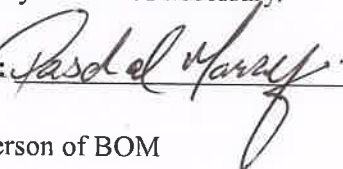
For Visitors, Contractors and other authorised Users, the School may restrict or withdraw access to ICT Resources or School Systems where necessary.

Where activity may constitute a criminal offence or create a serious safeguarding, data protection, cybersecurity or other legal or regulatory concern, the School may refer the matter to the appropriate authority.

The School may restrict, suspend or withdraw a User's access to ICT Resources or School Systems where necessary to respond to a breach or protect Users, School information, ICT Resources or School Systems.

10. Review of the Policy

The Policy will be reviewed every three years following its implementation and may be reviewed more frequently if deemed necessary.

Signed: 
Chairperson of BOM

Date: 22.10.2026.

Signed: 
Principal/Secretary to BOM

Date: 22.10.26

AI TRAFFIC LIGHT

Guidance for Ethical AI Use

Use this guide to decide when and how AI can support your learning.

GO!

AI AS AN ASSISTANT

Use AI here to support your ideas and learning.

Examples:

- Brainstorming ideas
- Generating ideas or topic suggestions
- Creating an outline or plan
- Checking spelling, grammar or punctuation
- Explaining a concept in simple terms (when you are stuck)

RULE: AI helps me start, but I do the work!

SLOW DOWN!

CHECK WITH YOUR TEACHER BEFORE USING AI HERE.

Examples:

- Summarising long articles or information
- Explaining difficult concepts in more detail
- Translating text
- Finding sources or information
- Getting feedback on your work

RULE: Always check with my teacher before using AI!

STOP!

NOT ALLOWED

These uses are not allowed.

Examples:

- Copying and pasting AI-generated text
- Having AI write my entire essay or assignment
- Presenting AI work as my own original work
- Using AI to get answers in tests or exams
- Creating or sharing inappropriate, harmful or offensive content

RULE: This is cheating and not my own thinking!

Always follow your teacher's instructions and our Acceptable Use Policy.

AI is a tool. You are in charge of your learning and your choices.

My brain is the master, AI is the tool.

Be responsible. Be respectful. Be honest. Be you.

ACCEPTABLE USE POLICY (AUP)

Our expectations for using technology at school

Technology helps us learn, create and connect.
Use it safely, responsibly and respectfully.

YOU CAN

- Use technology to support your learning and creativity.
- Communicate respectfully and positively with others.
- Use the internet to find, evaluate and share information responsibly.
- Follow your teacher's instructions and school rules.
- Speak up and ask for help if something doesn't feel right.

Technology is a privilege. Use it wisely to help yourself and others.

YOU MUST

- Look after school devices and report any damage or issues.
- Keep your passwords private and log out when you are finished.
- Protect your own and others' personal information and privacy.
- Be kind, respectful and inclusive in all online interactions.
- Follow copyright rules. Give credit when using others' work.
- Let a teacher know immediately if you see something inappropriate or upsetting.

We all have a responsibility to keep our school community safe and respectful.

YOU CANNOT

- Access or share inappropriate, harmful or illegal content.
- Bully, harass or be unkind to others online.
- Download or install software, apps or files without permission.
- Connect USB drives or other removable storage without permission.
- Take, create or share photos or videos without permission.
- Plagiarise, copy or present someone else's work as your own.
- Use technology for personal entertainment during class time unless given permission.

Misuse of technology can lead to loss of access and serious consequences.

YOUR RESPONSIBILITIES

- Use School ICT Resources and Systems for learning unless you have permission to use them for another purpose.
- Be respectful of others online and offline. Your words and actions matter.
- Keep information safe. Do not share personal, confidential or sensitive information (yours or others').
- Think before you post. Once online, it can be hard to remove.
- Follow the time limits and expectations set by teachers.

REMEMBER

- Be a positive digital citizen.
- Use technology fairly and responsibly.
- Protect your wellbeing and take breaks.
- Support others and report concerns.

When in doubt, ask a teacher!

When you use technology responsibly, you help create a safe, positive and productive learning environment for everyone.

Be respectful. Be responsible. Be you.