ICT Acceptable Usage Policy

St. Michael's College is committed to the ethical and moral use of all Information Technology (ICT). St. Michael's College is continually developing and managing the information security environment to comply with the highest standards. St. Michael's College is supportive of and committed to maintaining high standards of information security and views information security as essential to the long-term goals and strategic objectives of the College. St. Michael's College wishes to comply with all relevant legislative, regulatory and contractual requirements.

The purpose of the policy

The purpose of the policy is to define how electronic communications are managed in the College and the rights and responsibilities of those managing areas and all users.

Acceptable Usage Policy

This ICT Usage Policy applies to the students, employees and volunteers at St. Michael's College and all other persons offered access to College Information and Communication Technology (ICT) systems. (The term 'User' refers to all).

Aims

St. Michael's Acceptable Use Policy aims to ensure that students will benefit from learning opportunities offered by the school's digital resources. We aim to create a culture of responsibility and wish to stress the partnership between family, school and student. Access to digital resources is seen as educationally beneficial and a privilege. If the school AUP is not adhered to this privilege will be withdrawn and appropriate sanctions, as

outlined below will be imposed. St. Michael's is committed to developing a first-class digital learning environment as we recognise the benefits of digital technology in education. The College has developed a Digital Learning Plan for 2023/4. It is developing its strategy in line with the Dept. of Education Digital Strategy for Schools to 2027

School's Strategy

The school employs several strategies to provide digital learning opportunities and also reduce risks associated with the Internet. These strategies are as follows:

General

- Introduction of iPads for digital learning from 2023/4 as a pilot in 1st Year, moving towards all Junior Cycle students having one-to-one educational devices (iPad) by 2025/26.
- Internet sessions will always be supervised by a teacher.
- Filtering software and/or equivalent systems will be used to minimise the risk of exposure to inappropriate material.
- The school will regularly monitor students' ICT usage.
- Students and teachers will be provided with training in the area of Internet safety. Teachers can access training from Select Apple for Education in-house training, teacher peer training and Oide Technology in Education
- Uploading and downloading of non-approved software will not be permitted. Working with our Wi-Fi provider, the school has established a secure system, a password-protected staff Wi-Fi and Student Secure Wi-Fi for student iPad usage.
- Virus protection software will be used and updated regularly.
- The use of memory sticks or other digital storage media in school requires a teacher's permission.
- Teachers will be provided with student device surveillance software (e.g.) Apple Classroom, AB Tutor, etc.
- Students will not undertake any online actions that may bring the school into disrepute or harm themselves or others.
- The management team of the school have access to Google Administrator

facility to monitor usage and receive regular reports/alerts

- iPads are managed via Jamf and Apple Manager secure systems

Scope

This policy applies to all users of St. Michael's College's ICT resources, both on and off-site, within and outside of normal working hours. The policy covers the appropriate use of such technology and the College's right to log and monitor any such activity including details such as the content of emails, which sites are visited and what is downloaded. Each user is responsible for being fully aware of the ICT Usage Policy and its implications for personal conduct. As in all their work activities, users are required to use ICT resources in a reasonable, professional, ethical and lawful way.

General Principles of Acceptable Usage Policy

St. Michael's College's ICT systems, resources and associated applications are intended for activities that support the mission, goals and objectives of the College. This usage is encouraged and supported. The ICT systems, resources and associated applications are to be used in a manner consistent with the College's mission and values and as part of the normal duties of all persons offered access to the College's (ICT) systems.

The College's email accounts, Internet identifications and web pages should only be used for appropriate and sanctioned communications.

The use of the College's resources and associated applications may be subject to monitoring for security and/or network management reasons and as a result, users may also have their access and use restricted. At St. Michael's College use of internet-software is used to monitor access to websites. The distribution of any information through the Internet, email and any messaging systems through the College's network is subject to scrutiny by appropriate personnel.

It is the responsibility of each member of staff and user to protect the information or information assets under their direct control and to adhere to the established information security policies and procedures when conducting their duties. Breach of information security policy and procedures may result in disciplinary action up to and including dismissal/expulsion.

Users have a personal responsibility to report any information security incidents or suspected weaknesses to the Principal/Deputy Principal or any member of the ICT team at the first opportunity. Users are asked to report and look for assistance if they access material or receive an inappropriate message. They should contact any member of the school management team. All members of the College are reminded to not open suspicious emails they may suspect to be containing ransomware/malware.

Users must not access, download or send any material through ICT technology which:

- Is offensive or could give rise to offence being taken by a 'reasonable person'.
- Is illegal.
- Could bring the College into disrepute.

The use of all ICT systems, resources and associated applications are subject to Irish and European law and any illegal use will be dealt with appropriately through the College's disciplinary process.

St. Michael's College is committed to ensuring that it operates in compliance with the Data Protection Acts 1988 and 2003. St. Michael's College makes every effort to ensure that personnel information is maintained in a manner which is accurate, relevant and is held securely at all times. All those maintaining records on behalf of the College are asked to ensure that they adhere to the provisions of the Data Protection Acts and Data Protection Guidelines. The College retains the right to report any actual or potential illegal violations to the relevant State and other Authorities.

Individual Practice

Introduction of iPads 2023/4

Blended Learning Model: Use of one-to-one devices for students

From 2023/4 First Year Students have one-to-one iPad devices. These devices are managed via the Jamf Management system by Apple Select for Education. Each student is provided with their own managed Apple ID and password. Apps are pushed securely onto the managed environment. Teachers can monitor activity in the classroom via the Apple Classroom app. Application management is centralised
and student devices can be locked onto a specific working platform.
The iPads are administered by the College ICT administrator and managed by the Deputy Principal. Students must comply to the AUP and the devices are for educational purposes only.

Online and Digital Guidelines for Students

Online Browser usage

- Students will not intentionally visit Internet sites that contain obscene, illegal, hateful or otherwise objectionable materials.
- Students will report accidental access to inappropriate materials to the school authorities.
- Students will use the Internet for educational purposes only.
- Students will not use AI or Chat GPT-generated content to compose their written assignments.
- Students will not copy information into assignments and fail to acknowledge the source (plagiarism and copyright infringement).
- Students will never disclose or publicise personal information (their own or others) online.
- Downloading by students of materials or images not relevant to their studies is in direct breach of the school's acceptable use policy.
- Students will be aware that any usage, including distributing or receiving

information, school-related or personal, may be monitored for unusual activity, security and/or network management reasons.

Use of Email

- Students will use approved @stmc email accounts assigned for school use by the College.
- Students will not send or receive any material that is illegal, obscene, defamatory or that is intended to annoy or intimidate another person.
- Students will not reveal their own or other people's details, such as addresses or telephone numbers or pictures.
- Students will never arrange a face-to-face meeting with someone they only know through emails or the Internet.
- Students will note that sending and receiving email attachments is subject to permission from their teacher.

Internet Chat

- Students will only have access to chat rooms, discussion forums, messaging or other electronic communication forms that have been approved by the school for educational use. In general, the use of these forums will be blocked and discouraged in school. Email via the school account is the acceptable form of communication between parents, staff & students.
- Students will not use social media accounts via the school system, these will be blocked by the College firewall facility.
- Usernames will be used to avoid disclosure of identity.
- Face-to-face meetings with someone organised via Internet chat will be forbidden.

School Website

- The school website will be managed by a school website administrator who is a member of the College staff.
- The website will be regularly checked to ensure that no content compromises the safety of students or staff.
- Consent to appear on the school website and school social media is sought from new parents upon enrolment in the school. Students from whom parental consent has not been received, do not feature on the website or social media.
- Personal student information including home address and contact details will be omitted from school web pages.
- In line with data protection guidelines, new visitors to the school website are informed of the data retention policies and are given an opportunity to amend their own preferences prior to browsing.

Personal Devices

Students using their own technology in school, such as leaving a mobile phone turned on or using it in class, sending nuisance text messages, or the unauthorized taking of images with a mobile phone camera, still or moving is in direct breach of the school's acceptable use policy. **Students in years that do not have iPad access may be allowed to use their devices under supervision for educational purposes only.** Phones are not allowed for personal use in the school building, as per our Code of Behaviour.

Legislation

The school will provide information on the following legislation relating to use of the Internet which teachers, students and parents should familiarise themselves with:

- Data Protection (Amendment) Act 2003
- Child Trafficking and Pornography Act 1998
- Interception Act 1993
- Video Recordings Act 1989
- The Data Protection Act 1988
- The Data Protection Act 2018

Support Structures

The school will inform students and parents of key support structures and organisations that deal with illegal material or harmful use of the Internet.

Sanctions

Misuse of the Internet may result in disciplinary action, including written warnings, withdrawal of access privileges and, in extreme cases, suspension or expulsion. The school also reserves the right to report any illegal activities to the appropriate authorities.

Access and Passwords: Good practice would suggest the following guidelines

- **Password Protection:** Each user is issued ICT details (e.g. login/password for @stmc.ie Google Account) for their use and must not pass on log-in details/ passwords etc. to anyone other than an IT professional when appropriate. Passwords should never be shared (but disclosed to the ICT Coordinator when necessary) and should be changed at regular intervals and not be reused. Managers of computer systems are required to hold a record of all access passwords in an area at all times, in a secure location

Internet Access: Each person using the internet does so under their password and hence will have responsibility for illicit use of that password with or without their consent. Internet Access is conditional on the following additional rules being observed Where internet access is available to particular employees/persons the internet is for the College's business only. Users who in the opinion of management, have abused this, will be subject to disciplinary sanction. To access, download or send any indecent, obscene, pornographic, sexist, racist, defamatory or other inappropriate materials, as well as the circulation of such materials, will be a serious offence, which may result in expulsion or dismissal. This rule will be strictly enforced and is viewed as very serious with potential criminal liabilities arising there from. The Gardaí or other appropriate authority will be informed, where appropriate.

Software and Hardware: Users should not attempt to disrupt the computer system by interfering with software or hardware. No deliberate attempt must be made to introduce software of any kind, including games to the system without the expressed permission of

the ICT Coordinator

Data Storage: Where available, staff should save their work files on the local server to ensure that it is backed up by the server. In the instance of a local server not being available, staff must ensure that critical data is backed up by consulting with their manager and making appropriate arrangements for data backup. Staff are encouraged to store data safely in the @stmc.ie Google Cloud Drive or in Dropbox.

Moving Data Off-site / USB Keys: Users must show due diligence when transferring, carrying and using any electronic data off of the St. Michael's College systems (e.g.) working on home PCs. St. Michael's College has a legal obligation to protect its data content and cannot control data on personal PCs. Therefore, it cannot be emphasised strongly enough, that the use of USB / Memory sticks to transfer confidential information must be treated with great caution. The use of encrypted USB keys is highly recommended. All users must take appropriate precautions to preserve the security of the College IT systems, being aware of risks from ransomware / malware cyber threats.

Personal gain or profit: Users may not use the ICT system for unauthorised and unapproved commercial purposes or personal gain or profit.

Users should not subscribe to electronic services or other contracts on behalf of St. Michael's College unless with the express authority to do so.

Users will respect the rights of copyright owners. Copyright infringements occur when one inappropriately reproduces a work that is protected by a copyright. The use of photographic images or film on behalf of the College should respect copyright obligations and be appropriate for use, consistent with the ethos of the College.

Risk of Harassment Users will not use the ICT systems to access, download or send any material that could be found to be inappropriate or offensive by others, i.e., material that is obscene, defamatory or which is intended to annoy, harass or intimidate another person or advocates discrimination towards other people. This could be regarded as harassment or bullying and would be dealt with according to the Dignity at Work policy and disciplinary code.

Users will not use the ICT systems to access, download or circulate material that contains illegal or inappropriate material such as obscene, profane, objectionable or pornographic material or that advocates illegal acts or that advocates violence.

ICT facilities should not be used to make or post indecent remarks, proposals or any material which may bring the College into disrepute. **It is not permissible to advertise** or to otherwise support unauthorised or illegal activities.

Inappropriate Language: Users will not type, record or reproduce obscene, profane, lewd, vulgar, rude, inflammatory, racist, threatening or disrespectful language or images on the computer system. Information which could cause damage, danger or disruption will not be posted. Users will not knowingly or recklessly post false or defamatory information about a person, group or organisation. Users will not engage in defamatory or personal attack, prejudicial or discriminatory, that distress or annoy another person. Should students cause damage to the ICT system, they must bear the cost of repairs/replacement.

The use of email and other computer-based Communications:

There are risks attached to the sending of E-mails, therefore the following should be taken into account:

- A message may go to persons other than the intended recipient and if confidential or sensitive this could be damaging to the College.
- E-mail messages can carry computer viruses dangerous to computer operations generally.
- Letters, files and other documents attached to E-mails may belong to others and there may be copyright implications in sending or receiving them without permission.

- E-mail messages written in haste or written carelessly are sent simultaneously and without the opportunity to check or rephrase. This could give rise to legal liability on the College's part such as claims for defamation, etc.
- An E-mail message may legally bind the College in certain instances without the proper authority being obtained internally.
- It should be remembered that all personal data contained in E-mails may be accessible under Data Protection legislation and, furthermore, a substantial portion of E-mails to Government and other public bodies may be accessible under Freedom of Information legislation.
- E-mails should be regarded as potentially public information which carry a heightened risk of legal liability for the sender, the recipient and the organisations for which they work.
- To reduce the risks inherent in the use of E-mail the following guidelines are necessary:
- Users should only use approved e-mail accounts (i.e.) @stmc.ie on the school system for purposes related to their work at St. Michael's College.
- The use of BCC (Blind Carbon Copy) for internal communication is not permissible to prevent flame attacks.
- Particular care should be taken when sending confidential or commercially sensitive information. E-mail is neither a secure nor a private medium. If in doubt please consult a member of the IT team.
- Care should also be taken when attaching documents as they may give rise to the release of information not intended, therefore it is important to vet attachments. The ease with which files can be downloaded from the Internet increases the risks of infringement of the rights of others particularly the intellectual property and other proprietary rights. If in doubt please consult your manager.

- An E-mail should be regarded as a written formal letter, the recipients of which may be much wider than the sender intended. Hence, any defamatory or careless remarks can have very serious consequences as can any indirect innuendo. Inappropriate remarks whether in written form, in cartoon form or otherwise must be avoided, as should any remarks that could be deemed indecent, obscene, sexist, racist or otherwise offensive or in any way in breach of current legislation.

- Should you receive any offensive, unpleasant, harassing or intimidating messages via the E-mail you are requested to inform the Principal/Deputy Principal or any member of the ICT team.

- Any important or potentially contentious communication which you have received through E-mail should be printed and a hard copy kept. Where important to do so you should obtain confirmation that the recipient has received your E-mail.

- Documents prepared for your service users may be attached via the E-mail. However, excerpts from reports other than our own, if substantial, may be in breach of copyright and the author's consent ought to be obtained particularly where taken out of its original context. Information received from one service user / client should not be released to another service user / client without prior consent of the original sender - if in doubt consult your manager.

2) **The Use of Other Technologies / Social Media Websites or Applications**

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in the College is allowed.
- Staff must inform the ICT Coordinator if they wish to use any new web-based ICT program on the school systems.
- Staff should not give out their personal email addresses, or any social media addresses as a personal point of contact to students. All communication should be via College email @stmc.ie. Students should not access social media during school time and should not post any information about staff or students on public forums, social media or wider internet.

When using ICT systems, users must not represent personal opinions as those of the College. All staff and other users are instructed to use a disclaimer such as:

"The information in this e-mail is confidential and may be legally privileged. It is intended solely for the addressee. Access to this e-mail by anyone else is unauthorised. If you are not the intended recipient, you are notified that any disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited. Any views, opinions or advice contained in this e-mail are those of the sending individual and not necessarily those of the College. It is possible for data transmitted by e-mail to be deliberately or accidentally corrupted or intercepted. For this reason, where the communication is by e-mail, St. Michael's College does not accept any responsibility for any breach of confidence which may arise from the use of this medium."

Confidentiality

Notwithstanding the College's right to retrieve and read any electronic mail messages, such messages should be treated as confidential by other employees and accessed only by the intended recipient. Employees are not authorised to retrieve or read any e-mail messages that are not sent to them. Any exception to this policy must receive prior approval from DP/P or relevant ICT team member. However, the confidentiality of any message should not be assumed. Even when a message is erased it is still possible to retrieve and read that message. If any breach of our E-mail policy is observed then disciplinary action up to and including dismissal/expulsion may be taken.

Users must not upload, download or otherwise transmit commercial, unlicensed software or any other copyrighted materials that belongs to the College or external parties. Users must not reveal, publicise or disclose any information that might be in breach of the Data Protection legislation

Users must not reveal or publicise confidential or proprietary information that includes, but is not necessarily limited to, all types of educational or financial information, strategies and plans, databases and the information contained therein or any other information which is deemed the property of the College. Send confidential emails without applying appropriate security protocols.

Security

- All digital devices must have virus detection software installed; users must not attempt to investigate virus programmes themselves.
- To prevent computer viruses from being transmitted, care must be exercised by users in the downloading of material. It should be from a reliable source and the user must not seek to avoid the standard virus protection measures implemented by St. Michael's College. Staff must ensure that virus protection on personal devices is up-to-date to avoid bringing viruses into the school.
- Only software that is authorised, licensed and approved must be installed on St. Michael's College equipment, and licence agreements are complied with.
- Users must not intentionally interfere with the normal operation of the College ICT systems, resources and associated applications. This includes the distribution of computer viruses and sustained high-volume network traffic that substantially hinders other users of the network.
- It is not permitted to examine, change or use another person's username, password, files or outputs for which no explicit authorisation has been given.
- Care must be taken that mobile devices are secure at all times and that no confidential data is stored on them. They should be locked away when not in use and user –IDs or passwords should not be stored with the device.
- Care must be taken that all documents and computer media are disposed of securely at the end of their life, shredded or sent to secure disposal as appropriate.
- All computers in the offices of the College should be monitored regularly to ensure that they are being used in accordance with the stated policy. Where there is any suspicion or doubt a person with specialist knowledge of computer hardware and software should be asked to assess the purposes for which the computer has been used. The College employ a professional ICT company to offer support and guidance regarding cyber security.

Safeguarding Children

Students should be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. Ensuring students are aware of the SMART rules and are aware of how to use the Internet effectively is the responsibility of all teachers. Teachers must be aware of the regulations regarding the use of Web 2 applications and email and seek to protect students and themselves in this regard.

- Where possible, if a computer is used by more than one person, each person should be obliged to have a unique username and password. All users should sign out of their email and Google Spaces when finished using a device. The school will work with their ICT providers to ensure that there is appropriate security protection on the College servers

- If there is any question as to the security of a PC or other device, a person with specialist knowledge of computer hardware and software should be asked to assess the purposes for which the computer has been used.

- As technology is a fast-moving area, St. Michael's College should continuously evaluate the possible ways that students communicate with staff, volunteers and each other, such as via the internet, mobile phones, email using digital and other electronic or information technology.

- It is important to develop guidance to reduce the risks to children that may arise in the course of their use of technology. Such risks include:
    - Online grooming of minors for exploitation
    - Experiencing or perpetrating bullying
    - Accessing or being exposed to inappropriate or harmful material
    - Having their contact details accessed and circulated
    - Having personal images uploaded and used without consent.

All personnel and other users must adhere to this ICT Usage Policy or risk disciplinary action in line with the College's codes of conduct. The College should develop a Form of Acceptance (see sample below) which should be signed by each user. This policy will be reviewed and updated as required

FORM OF ACCEPTANCE

Name of Student: _____

Class/Year: _____

Student

I agree to follow the school's Acceptable Use Policy on the use of the Internet. I will responsibly use the Internet and obey all the rules explained to me by the school.

Student's Signature: _____ **Date:**_____

Parent/Guardian

As the parent or legal guardian of the above student, I have read the Acceptable Use Policy and grant permission for my son to access the Internet. I understand that Internet access is intended for educational purposes. I also understand that every reasonable precaution has been taken by the school to provide for online safety but the school cannot be held responsible if students access unsuitable websites. Occasionally, photographs or videos may be taken of students in the course of their school work or extra-curricular activities. These may be published on the school website. I understand and accept the terms of the Acceptable Use Policy relating to publishing student's work on the school website

Parent/Guardian Signature:_____

Date_____