ICT Acceptable Use Policy

ICT Acceptable Use Policy

PURPOSE

This policy establishes best practice for the use of Information and Communication Technology (ICT) within St Michael's College.

SCOPE

This policy applies across St Michael's College and includes:

- All information processed, stored, and transiting ICT facilities.
- All ICT equipment, hardware and software used in the conduct of the ICT function within St Michael's College.

This policy applies to the following:

- All staff and students within St Michael's College
- All consultants, contractors, volunteers, visitors, agents and authorised users accessing St Michael's College ICT systems and applications.

DEFINITIONS

SMC - refers to St Michael's College

ICT - Information and Communications Technology is a term that includes any facilities used to compute, communicate and to store information electronically. This may include and is not limited to desktop, laptop, and tablet computers, computer servers, electronic storage devices, network and telecommunications equipment and associated software. ICT resources include, but are not limited to, mobile and wearable devices, AI-enabled platforms, generative AI tools, cloud-based services, and AI functions embedded within approved software applications such as AI-assisted drafting in word processing or email tools.

Staff - refers to any employee of SMC, including contractors, casual staff and outsourced staff provided with contact or access to SMC provided ICT facilities.

POLICY STATEMENT

ACCEPTABLE USE

All individuals who access, use or otherwise engage SMC ICT resources are required to:

- Respect the rights of all individuals, including other users.
- Only use or modify SMC ICT resources for authorised purposes and not in breach of relevant laws, regulations and/or professional contractual obligations.
- Not use SMC computer or network equipment for personal, purposes beyond reasonable use, or in a way that may adversely affect SMC or conflict with its values.

- Not access, distribute, store or display illegal, pirated or offensive material.
- Not use SMC computer or network equipment for unauthorised personal financial or commercial gain.
- Not misrepresent the views of SMC via use of SMC ICT resources.
- Not conduct activities that consume excessive network bandwidth.
- Report suspect or actual security breaches to SMC ICT Support Team in a timely manner.
- Maintain the security and confidentiality of information gathered or collected by SMC in accordance with the SMC Privacy Policy.
- Adhere to all policies, procedures and guidelines as published and updated periodically.
- Only use software, applications, and AI platforms that have been approved by the College for school-related purposes. The use of unapproved or insecure external platforms in ways that involve College data, student information, or school-related work is prohibited.
- Handle personal or sensitive information in accordance with the data classification framework established in the SMC Responsible Use of Artificial Intelligence Guidelines, which sets out the specific conditions under which different categories of information may or may not be used with AI tools. This framework governs what data can be entered into any AI platform, whether College-approved or external.
- Be aware that data entered on external or cloud-based services, including AI platforms not operated by SMC, may be stored, processed, retained, or used by those third parties. Users must not use unapproved external platforms for any purpose that involves College-related data and should exercise caution even when using approved platforms to understand how their data is handled.
- Ensure that where ICT resources are used to collect, record, or process personal information about students, staff, or families, including through AI-enabled systems, appropriate consent is obtained in accordance with the SMC Privacy Policy and applicable state and federal legislation.
- (**Students**) Not use ICT resources, including AI tools, to produce or submit work that misrepresents their own learning, knowledge, or effort. Any use of AI in the preparation of assessment tasks must comply with teacher instructions and relevant academic integrity policies.
- Seek the consent of all parties to film and record meetings. This applies to any mobile device including wearable or recording-capable device, such as smart glasses, AI-enabled eyewear, wearable cameras, smart watches or similar technologies capable of recording, livestreaming or transcribing. All users in this policy's scope must not wear or operate such devices in a way that records, livestreams or transcribes students, staff or other members of the College community while on College premises or at College events, without the prior permission of the College and of the individuals concerned. Where a device is worn for medical, accessibility or assistive reasons, parents are asked to advise the College in advance so appropriate arrangements can be made. Further detail is set out in the College's Social Media Policy and Mobile and Wearable Devices Policy.

SECURE SYSTEM ACCESS AND USE

To protect access to SMC ICT resources, individuals are required to:

- Select long and strong passwords that adhere to parameters as defined in the Access Management Policy.
- Not share SMC-provided or self-selected passwords with other individuals.
- Keep personal and SMC provided systems, used to access SMC information, free from known vulnerabilities by keeping up to date with vendor provided security updates.
- Maintain operational and up to date antivirus on personal and SMC provided systems used to access SMC systems or information.
- Securely store passwords that provide access to SMC systems or information.
- Only use the accounts provided by SMC for their own individual use.
- Only use the accounts provided by SMC for SMC related purposes.
- Not bypass or attempt to circumnavigate SMC's security controls or protection mechanisms.

- Not introduce malicious software such as viruses, worms, ransomware or trojans into the SMC environment.
- Not use hacking tools (including sniffing, scanning, password guessing or exploitation) when accessing, using or otherwise engaging with SMC ICT resources.
- Not reuse SMC passwords for private use applications.
- Ensure that personal devices used to access SMC systems, information, or approved platforms — including AI tools — are maintained with up-to-date antivirus software and operating system security updates, consistent with the requirements of this policy.

MONITORING AND COMPLIANCE

- SMC will monitor its ICT resources for compliance with this policy and breaches of this policy constitute misuse of SMC information and information systems.
- The ICT Acceptable Use Policy – provides some examples of activities that constitute misuse of ICT resources. If misuse of ICT resources is detected or suspected, relevant disciplinary provisions including the revocation of system privileges, disciplinary action up to and including dismissal may be invoked.
- Breaches of this Policy will be managed in accordance with the relevant College policies, procedures and codes of conduct applicable to staff, students, contractors, volunteers, visitors or other users of SMC ICT resources. Appropriate disciplinary, administrative or remedial action may be taken, depending on the circumstances and seriousness of the breach.
- SMC may refer serious matters or repeated breaches the appropriate external authorities which may result in disciplinary and/or civil and/or criminal proceedings.
- SMC has a statutory obligation to report illegal activities or corrupt conduct to appropriate authorities and will cooperate fully with the relevant authorities.
- To the extent allowed by law, SMC is not liable for loss, damage or consequential loss or damage arising directly or indirectly from the use or misuse of any ICT resources.

RELATED POLICIES, PROCEDURES AND SUPPORT DOCUMENTS

This policy is to be read in conjunction with the following documents:

- SMC Cyber Security Policy
- SMC Acceptable Use Guideline
- SMC Privacy Policy
- SMC Generative AI Policy
- SMC Responsible Use of Artificial Intelligence Guidelines
- SMC Mobile and Wearable Devices Policy
- SMC Community Charter

REVISION RECORD

Policy Owner	Business Manager
Approval Authority	ICT Committee
Reviewed	New Policy September 2026
Next Review Date	September 2029
Risk Rating	Moderate