ICT Acceptable Use Guideline

ICT Acceptable Use Guideline

PURPOSE

This guideline provides a practical direction for staff and students on the safe, responsible and effective use of ICT facilities within St Michael's College.

SCOPE

This guideline 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.

This guideline supports the SMC Acceptable Use Policy.

DEFINITIONS

SMC - refers to St Michael's College

ICT Facilities - includes and is not limited to computer systems, cloud-based resources, data networks, wireless infrastructure, Internet connections, computers, laptops, smart phones, applications, printers and other means of electronic communication.

ICT - Information and Communications Technology is a term that includes any facilities used to compute, communicate and store information electronically. This may include and is not limited to desktop, laptop, tablet computers, computer servers, electronic storage devices, network and telecommunications equipment and all associated software and all supporting peripheral devices. ICT resources also include AI-enabled platforms, generative AI tools, and cloud-based AI services, whether provided by the College or accessed externally for College-related purposes.

Staff – refers to **all** staff employed by St Michael's College, including casual employees and contractors.

AI Tools and Cloud Based AI Services - refers to any artificial intelligence platform, application, or service accessed via the internet or cloud infrastructure, whether provided by the College or accessed externally. This includes mobile or wearable devices, generative AI tools, AI-assisted features embedded within approved software, and any AI-enabled service that processes or generates content in response to user

input. For the purposes of this guideline, these are considered ICT resources and subject to all obligations set out in this guideline and the SMC ICT Acceptable Use Policy.

STANDARDS AND APPROPRIATE USE GUIDELINES

Acceptable Use of ICT Facilities

All users must use ICT facilities ethically, lawfully, respectfully and in a way that aligns with the College's values.

Incidental Personal Use - Incidental personal use is permitted if the use:

- Adheres to SMC policies and standards.
- Does not hinder the staff member's productivity and in the case of a student does not interfere with student learning, safety or wellbeing
- Is approved by an appropriate authority such as line manager, Principal or delegate as required.
- Is legal and complies with SMC regulatory and contractual requirements.

Appropriate Use - Use of ICT facilities requires that persons:

- Access to College systems, records and information must not be provided to any unauthorised person, including family members, friends or students. Confidential College information must only be accessed, used and shared for legitimate College purposes and in accordance with the user's role and responsibilities.
- Access only the information necessary in the execution of their duties. Any access rights not required are to be reported through management to the relevant IT Support via email: itsupport@smc.sa.edu.au
- Recognise obligations implied and explicit regarding the maintenance of confidentiality, security, integrity and privacy of information for which they either have access to or have responsibility for.
- Comply with all applicable legal and regulatory obligations, including those relating to privacy, copyright and software licensing.
- **Maintain secure password practice:**
  - Maintain a secure password known only to themselves i.e. no password sharing.
  - Maintain discrete passwords for individual systems, using a password management system as necessary and as recommended or endorsed by an appropriate ICT authority.
  - Use passwords that comply with the SMC Access Management procedure.
  - Notify the IT Department immediately if suspicious activity regarding access or passwords is suspected.
  - Use multifactor authentication as implemented and in accordance with SMC access management (password and passphrase) requirements.
  - Use only the email account allocated to yourself. Use of another's email account is not permitted and may result in disciplinary action.

- Maintain awareness of privacy and legal obligations in relation to still and video photography. No images are to be taken without the express consent of the individuals concerned.
- 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.
- Maintain awareness of the SMC cyber security policy, procedures and expectations to maintain high standards of security.
- Maintain awareness of the SMC Generative AI Policy, procedures and expectations.
- Report evidence of, or suspicion of unauthorised access, use and other suspicious activity in the use of ICT assets and information assets to the IT Department.
- Report access to inappropriate material, accidental or otherwise to IT Support/ICT Manager.
- Ensure the safe keeping of all equipment and the data stored within the ICT provided in the course of your work.
  - Staff are required to report any loss of equipment as soon as practical.
  - Equipment to be safely transported, not left unattended and not visible during transit. For example, store equipment in car boot, not on a seat or car floor.
- Users of SMC ICT facilities are not permitted to download or install software unless it has been approved by the IT Manager and declared safe and licenced for use within SMC.

Unacceptable Use of ICT Facilities

Inappropriate activity includes that which:

- Is illegal or contrary to regulatory obligations.
- Seeks to gain unauthorised access to any resource or entity, including another's email account and/or system resources.
- Without authorisation destroys, alters, dismantles, disfigures, prevents rightful access to or otherwise interferes with the integrity of computer-based information and/or information resources.
- Transmits or causes to be transmitted, communication that is offensive or threatening, constitutes harassment, discrimination, vilification, defamation or bullying.
- Deliberately accesses, views, downloads, forwards any offensive information or material that is illegal, abusive, of a sexist, racist, or offensive nature including extremist, intolerant, pornographic, profane or is contrary to the generally accepted standards for the use of ICT facilities.
- Transmits or facilitates the transmission of unsolicited email, otherwise known as spam.

- Contravenes SMC licence obligations and agreements.
- Transmits or accesses sensitive, private or confidential information externally unless it is encrypted or otherwise protected using methods approved by the IT Department.

MONITORING AND COMPLIANCE

To ensure compliance:

- SMC entities will implement an acceptable use agreement as a condition of granting access to ICT facilities. A checklist and templates for such agreements are included as Appendices.
- All users of SMC provided ICT facilities will, by implication, accept that authorised IT staff will monitor activity by automated and manual means to ensure compliance and the highest levels of security are maintained.
- SMC will provide IT staff tools to proactively protect ICT facilities. Protections will include but are not limited to the provision of system wide threat protection solutions, alerting and monitoring.

In addition to these technical protections, adherence to the principles in this guideline strengthens the level of protection required and expected.

RELATED POLICIES, PROCEDURES AND SUPPORT DOCUMENTS

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

- SMC Cyber Security Policy
- SMC ICT Acceptable Use Policy
- SMC Privacy Policy
- SMC Generative AI Policy
- SMC Responsible use of Artificial Intelligence Guidelines
- SMC ICT Access Management Procedure
- SMC Community Charter
- SMC Mobile and Wearable Devices Policy

REVISION RECORD

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

Appendix A.
Checklist of items to be covered in Acceptable Use Agreements.

CHECKLIST OF MATTERS TO BE COVERED IN SCHOOLS' ACCEPTABLE USE AGREEMENTS

Exact wording and concepts to be adapted to suit the age and development of the relevant students in each School context.

1.	**Scope of Agreement**: with particular emphasis on use of personal devices at school, and out of hours conduct. This Agreement covers: ▪ all users of ICT within the College ▪ all use of school ICT facilities ▪ all use of personal ICT devices to access the school network or facilities ▪ conduct both during and outside of school hours.	☐
2.	**Acceptable Conduct**: ▪ conduct consistent with the Catholic & Lasallian ethos. ▪ behave ethically and responsibly in all dealings with others. ▪ observe obligations regarding confidentiality and privacy. ▪ select and maintain a secure password and ensure you do not provide the password to anyone else. ▪ restricted use of devices that record others or take photos. ▪ report any suspicions of unauthorised or inappropriate access to the College. ▪ treat equipment with care. ▪ physical control and safe keeping of devices supplied to them by the school.	☐
3.	**Unacceptable Conduct** ▪ send or publish any statement, image or other material that is offensive or threatening, or could constitute harassment, discrimination, vilification, defamation or bullying. ▪ knowingly access, download, store, send or publish any material that is pornographic. ▪ do anything that you know, or reasonably suspect could contravene the law, including without limitation downloading material in breach of copyright. ▪ send or help to send unsolicited bulk email (spam). ▪ attempt to gain unauthorised access to anyone else's account or user information or otherwise attempt to defeat any security controls. ▪ open or download any attachment, or access any link, that you reasonably suspect may contain a virus, malware or other computer contaminant. ▪ install unlicensed or non-approved software onto any supplied computers or communication devices. ▪ use ICT Facilities to cheat or plagiarise. ▪ use ICT Facilities to store or download files for personal use.	☐
4.	Staying Safe Online Reporting to an adult if a student accesses a website or sees something online that makes them feel uncomfortable	☐
5.	Specifics of what to do in the event of cyberbullying (victims and bystanders)	☐
6.	**Personal Devices** Personal ICT devices that access material on the school network and services: ▪ must be protected with a secure password. ▪ may be monitored by the College and/or SMC personnel. ▪ must be provided to the College authorities for the purposes of assisting the authorities to determine whether inappropriate conduct has occurred. ▪ usage of personal devices must comply with guideline statements as if the equipment was supplied by the school. ▪ Must permit the College to manage access to SMC information.	☐
7.	Students may use ICT facilities for incidental personal use, provided such use is minimal and does not interfere with the performance of their learning.	☐
8.	Students are encouraged to collaborate within the system; however, this should be done in a safe manner. Students should obtain a teacher's permission prior to establishing contact with participants not associated with their school. Teachers should record any approvals granted for external collaboration.	☐
9.	When posting material in social media forum students should be reminded that such activity may be considered public, not private.	☐
10.	Consequences of breach of this agreement may result in loss of privileges including loss of access to ICT facilities or further disciplinary procedures as appropriate.	☐

Appendix B. Sample Student Acceptable Use Agreement.



This User Agreement sets out the terms on which you may access information and communication (ICT) facilities provided by the school.

By signing this Acceptable Use Agreement, you (including parents/guardians in the case of students under 18 years) are agreeing to the terms set out in this Acceptable Use Agreement, including the consequences of any breach of the terms.

1. Privacy Consent

Information that you transfer or store using the school's computing services may have implications for Privacy and you are reminded to read and understand the school's Privacy policy.

2. Acceptable Use

You agree that you will comply with all requirements as set out in this Agreement, and any acceptable use documentation that may be provided to you by your school.

3. Monitoring

You agree that authorised St Michael's College staff can and will monitor your use of ICT facilities to ensure compliance with acceptable use guidelines and practices as defined and communicated to you.

4. Suspension or termination of use and other consequences

Inappropriate use of ICT services and facilities may result in the termination of access. Disciplinary consequences may also apply.

5. Agreement and Consent

I, the student named below, hereby agree to comply with all requirements as set out in this Agreement and in the Acceptable Use Standard and all other relevant laws and restrictions in my access to the various ICT resources through the St Michael's College network.

NAME: _____ CLASS: _____

SIGNATURE: _____ DATE: _____

Parent/Guardian Consent (for students under 18 years of age)

As the parent or legal guardian of the student named above, I consent to the student accessing the various information and communication technology resources through the school and) on the terms set out in this Agreement and related documentation provided.

NAME: _____ DATE: _____