Subject: **ICT ACCEPTABLE USE POLICY** Covers: **ALL STAFF AND STUDENTS, INCLUDING VOLUNTEERS AND CONTRACTORS**	Policy No: ICT2 – Version 6 Effective: January 2013 Revised: June 2024 Review Date: June 2027

Purpose:

The purpose of this Policy is to ensure that all use of School Information, Communications and Technology (ICT) resources is legal, ethical and consistent with the aims, values and objectives of the School and its responsibilities to the students in its care. The School has the dual responsibility to maximise the benefits of these technologies, while at the same time minimising the risk. The primary purpose of these technologies is to provide access to the vast number of online and local resources that support the School and its students in achieving strong learning outcomes.

ICT resources must be properly and efficiently used. ICT resources are not to be used for inappropriate activities for example, pornography, fraud, defamation, breach of copyright, unlawful discrimination or vilification, harassment, including sexual harassment, stalking, privacy violations and illegal activity, including illegal peer-to-peer file sharing.

Scope:

This Policy applies to all users of Collegiate ICT resources regardless of work location and applies to all aspects of use of all ICT resources, for example:

- All devices such as;
    - Computers (Desktops, Laptops, Tablets, etc) including BYOD devices;
    - Storage devices such as USB Cloud Storage and Network Folders;
    - Cameras; and
    - Audio Visual equipment.
- Publishing and browsing on the internet;
- Downloading or accessing files from the internet or other electronic sources;
- Email;
- Electronic bulletins / notice boards;
- Electronic discussion / news groups;
- Blogs and Wikis;
- Social networking;
- File transfer;
- File storage;
- File sharing;
- Video conferencing;
- Streaming media;
- Instant messaging;
- Online discussion groups and chat facilities;
- Subscriptions to list servers, mailing lists or other like services;
- Copying, saving or distributing files;
- Viewing material electronically; and
- Printing material.

Background:

The values we promote at St Michael's Collegiate School include excellence, creativity, diversity, meaning, ethical behaviour, and resilience. Our mission states that we respect all people and model and teach behaviours that embrace our values. The policy as set is based on these core values.

Exemplary behaviour is expected of everyone in our community at all times. Our services are monitored and where breaches of this agreement undermine the core values of the School and the safety of the learning environment, either through our set of services or 3rd party services, the School expects community members to take responsibility for their actions and restore any damage done.

Policy:

OBLIGATION OF ACCEPTABLE USE

Users are expected to use Collegiate's ICT resources in a responsible, ethical and legal manner, demonstrating respect for others, and an appreciation of the right to learn. The use of our resources must be consistent with the educational objectives of the School. Violation of any of these provisions may result in disciplinary action.

- The School's ICT resources must not be used to download, display, print, save or transmit material that would normally be considered offensive except in the context of a formal educational lesson.
- No attempt to perform malicious acts effecting either the School or a 3rd parties network must be made.
- The School's ICT resources must not be used for personal financial gain. Gambling and advertising are not permitted.
- Placing of unlawful information on the School's ICT resources is not permitted.
- Use appropriate language, common rules of courtesy and respect, and avoid all forms of harassment when communicating via the School's ICT resources.
- The use of any data provisioning devices / services other than those provided by the School, such as mobile hotspots, is prohibited.
- Use of the computer labs is restricted to those times when a supervising teacher is present.

ELECTRONIC COMMUNICATIONS

Electronic communications created, sent or received using Collegiate email systems are the property of Collegiate, and may be accessed by an Authorised Person in the case of an investigation, including in relation to investigations following a complaint or investigations into misconduct. Electronic communications may also be subject to discovery in litigation and criminal investigations. All information produced on computer, including emails, may be accessible during an investigation or at the direction of the Principal. Please note that email messages may be retrieved from back-up systems and organisations, their employees and the authors of electronic communications have been held liable for messages that have been sent.

Electronic communications should not be used to the disclose personal information of another except in accordance with the School's Privacy Policy or with proper authorisation. The Privacy Act requires employees and the School to take reasonable steps to protect the personal information held by the School from misuse and unauthorised access. In order to comply with the School's obligations under the Privacy Act, employees are encouraged to use the blind copy option when sending emails to multiple recipients where disclosure of those persons' email addresses will impinge upon their privacy. Employees should familiarise themselves with the Australian Privacy Principles ("APPs") and ensure that their use of email does not breach the Privacy Act or the APPs.

Electronic communication is not a secure means of communication. While every attempt is made to ensure the security of the School's ICT resources, users must be aware that this security is not guaranteed, particularly when communicated to an external party. The sender should consider the confidentiality of the material they intend to send when choosing the appropriate means of communication.

COPYRIGHT AND INTELLECTUAL PROPERTY

Copyright and licensing agreements must be respected at all times. A user must not be involved in any activity which breaches copyright or licensing agreements, including but not limited to activities such as illegally copying material in any format, copying software, downloading copyrighted video or audio files, using material accessed on the internet in order to plagiarise, or illegally using unlicensed products. It is the user's responsibility to know the laws pertaining to copyright.

Do not plagiarise. Acknowledge any material which you reproduce or use in any way, from any source and you must adhere to the School Policy on Plagiarism.

PRIVACY AND PERSONAL SAFETY

There is always a risk of false attribution of breaches of this Policy. It is possible that communications may be modified to reflect a false message, sender or recipient. In these instances, an individual may be unaware that he or she is communicating with an impostor or receiving fraudulent information. If a user has a concern with the contents of a message received or the identity of the publisher of the electronic information, action should be taken to verify their identity by other means. If a user believes an electronic communication has been intercepted or modified, the line manager or Principal should be informed.

Users are accountable for all use of ICT resources that have been made available to them and all use of ICT resources performed with their User ID. Users must maintain full supervision and physical control of ICT resources, including notebook computers, at all times. User IDs and passwords must be kept secure and confidential. Users must not allow or facilitate unauthorised access to ICT resources through the disclosure or sharing of passwords or other information designed for security purposes.

Collegiate staff must ensure that all ICT resources containing sensitive information, such as staff notebook computers, are only accessed by themselves and other Collegiate staff members. Students, family members, volunteers, contractors and other parties are not authorised to access ICT resources containing sensitive information. Unauthorised access of such resources must be reported to the Director of ICT.

Users must not identify, discuss, photograph or otherwise publish personal information or opinions about the School, staff or fellow students. The School holds a strong position in protecting the privacy of all in our community. No person may publish or upload images of members of the Collegiate community without their permission. No person may publish a picture of a member of the Collegiate community that would enable identification without the expressed permission of that person or their authorised representative and the School. Examples include wearing a Collegiate uniform, displaying a Collegiate badge.

MONITORING

Collegiate ICT resources may be accessed or monitored by Authorised Persons at any time without notice to the user. This includes, but is not limited to, use of School email systems and other electronic documents and records. Authorised Persons may access or monitor the records of ICT resources for operational, maintenance, compliance, auditing, legal, security or investigative purposes. For example, electronic communications, sent, received or forwarded using School ICT resources, may be accessed and logs of websites visited using ICT resources may be generated, examined and monitored.

If at any time there is a reasonable belief that ICT resources are being used in breach of this Policy, the Principal or line manager of the person who is suspected of using ICT resources inappropriately may suspend a person's use of ICT resources and may require that the equipment being used by the person be secured by the Principal or line manager while the suspected breach is being investigated.

In the event that the School chooses to access a device utilised by a user, this access will not be restricted to information created or accessed at school or using school ICT resources. For clarity, the School reserves the right to examine a device in its entirety, including internet history and all files regardless of where, when or how they were created. This applies to both BYOT and School provided devices.

DATA SECURITY AND STORAGE

Confidential data must not be stored on external or portable drives or on personally owned devices. Users must consider security requirements of all School related data they create and access. If data is confidential, private or intellectual property requiring protection, it must be handled to avoid unintended disclosure. If losing data would incur a high cost or impact, it must be handled to avoid accidental loss.

Data storage solutions provided by the School are suitable for storing both confidential and valuable data. These solutions are accessed via the network, have authentication and access controls, and provide a high level of protection from data loss by maintaining copies in multiple sites and use highly redundant technology. Current solutions are referred to as admin file shares, home drives (H drive).

It is not sufficient to rely on storage devices in desktops, laptops, external / portable drives, tablets and telephones to store valuable data. All valuable data must be primarily stored (or have a current copy stored) on School storage. It is common for user devices to fail and cause loss of all data stored on the device. Be aware that the hard drive, desktop and 'my documents' folders are not automatically backed up. Users must maintain current copies of valuable data on enterprise storage systems.

In the event that users do not comply with policy and as a result the School may lose valuable data, the School may elect, at is discretion, to pass on the data recovery costs to the non-compliant user.

Users must not store or backup confidential or valuable School data with externally hosted services other than where provided through and approved by the School. This is limited to the School owned and provisioned One Drive for Business Account.

Users must seek approval from the Director of ICT before signing themselves or others up to, or using any non-approved cloud services with their School devices and credentials. The Director of ICT will, upon approval, add the service to the School Cloud Services Register and provide guidance on what personal details may or may not be uploaded to the cloud services.

BRING YOUR OWN TECHNOLOGY (BYOT)

BYOT refers to devices that are owned by an individual, not the School and are used to access school ICT resources. All aspects of this policy apply regardless of if a user is utilising a BYOT device or school supplied / mandated device. This includes the securing and investigating of devices as per the above clause. In all cases of BYOT devices, the device must be the property of the student, parent who is agreeing to this policy or staff member. It is strictly prohibited for any member of the community to utilise a BYOT device to access ICT resources of which they, or their parent who is agreeing to this policy, is not the sole owner.

Junior School Students

The School provides Junior School students access to technology through the Junior School iPad program. As such, Junior School students are prohibited from bringing and utilising any BYOT devices to school. In rare circumstances, permission may be granted by the Head of Junior School and Director of ICT for students to use BYOT devices for a specific purpose. Devices that are not approved will be confiscated by the School and returned to the parents of the student as soon as practical.

Middle School Students

Middle School students are required to participate in the Middle School Prescribed Device Program. As such, Middle School students are prohibited from bringing and utilising any BYOT devices to school. In rare circumstances, permission may be granted by the Head of Middle School and Director of ICT for students to use BYOT devices for a specific purpose. Devices that are not approved will be confiscated by the School and returned to the parents of the student as soon as practical. During Year 8, when the School Prescribed Device is no longer meeting student requirements, a BYOT option is available with approval from the Director of ICT.

Senior School Students
Students in Years 9 to 12 participate in our BYOT program. Senior School students are required to bring a charged and working device to school each day. This device can be of their choosing but must have an operating system that is either Windows 7 or later or OS X 10.7 or later. The device must also have wireless connectivity. The School recommends that device should have at least an 11inch screen.

Staff & Other Community Members
Staff & Other Community Members may utilise BYOT devices at school. All aspects of this policy apply regardless of if a staff or community member is utilising a BYOT device or School provided device.

Support for BYOT Devices
BYOT Support is afforded to users who utilise their own technology at school. This support will include basic hardware troubleshooting and fault diagnosis and basic software configuration. The repair of any hardware faults is the responsibility of the user, and fault diagnosis is limited to the point where a rebuild / restore of the machine is required.

EXEMPLARY BEHAVIOUR
Exemplary Behaviour is expected at all times. When using the School's network, all users should conduct themselves as representatives of the School community as a whole.

BREACH OF AGREEMENT
The School will see any breach of this agreement as damaging a student, staff member or community member's relationship with the School. This will result in their access rights being revoked until they have restored their relationship with the School. At this point the School will invite the user to make this commitment again.