



St Michael's Collegiate CyberSafety Policy Agreement 2017

Collegiate's information and communication technologies are provided for educational, communication and research purposes for all members of the School community. 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.

Information and communication technologies includes, but is not limited to, computers (desktops, notebooks, tablets, PDA's) storage devices (USB and flash memory devices, CDs, DVDs, floppy disks, iPods, MP3 players), cameras (such as webcams, video or digital) all types of mobile phones, video or audio players/receivers (such as portable CD and DVD players) data provisioning services (school delivered internet services, personal / 3rd party data services), telephony services (either delivered by the school or personal / 3rd party services and any other similar technologies) and wearable technologies (Google Glass, Smart Watches, etc). 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.

OBLIGATION OF ACCEPTABLE USE

Users are expected to use Collegiate's information and communication technologies, ICT equipment/devices, network infrastructure and internet services 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 information and communication technologies, ICT equipment / devices, network infrastructure and Internet services 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 affecting either the School or a 3rd parties network must be made (this includes but is not limited to port scanning, ip scanning, mac spoofing, DOS attacks/storms, brute force attacks, use of key loggers, network sniffing, installation of rogue access points, use of technology that disturbs the delivery of wireless services).
- The School's information and communication technologies, ICT equipment /devices, network infrastructure and internet services must not be used for personal financial gain. Gambling and advertising are not permitted.
- Placing of unlawful information on the School's information and communication technologies, ICT equipment /devices, network infrastructure and Internet services is not permitted.
- When communicating via the School's ICT equipment / devices resources, use appropriate language, common rules of courtesy and respect, and avoid all forms of harassment.
- The use of any data provisioning devices/services other than those provided by the school is prohibited.
- The use of privately owned ICT equipment / devices other than data provisioning devices on the School site or network, or at any other school related activity must be appropriate to the School environment. This includes any images or material present/stored on privately owned ICT equipment/devices brought onto the School site or at school related activities.
- Publically hosted social internet sites must not be used during lessons or other formal school activities.
- The sending of chain letters or other unsolicited mail which would cause congestion on the network is not permitted.
- Use of the computer labs is restricted to those times when a supervising teacher is present.
- No person is permitted to use the Collegiate resources until she / he has returned a signed statement that they have read and agreed to the conditions of the St Michael's Collegiate CyberSafety Policy Agreement.

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.
- Copying or sharing software is not permitted.

PRIVACY AND PERSONAL SAFETY

- The privacy of others must be respected at all times.
- Sharing of network usernames and passwords is deemed as malicious activity and prohibited.
- Use of the internet and email carries the risk of bringing you into contact with individuals who may be unfriendly, rude or exploitative. Do not reveal personal details about yourself to strangers.
- No students may 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

- The School will exercise its right to monitor the use of the School's ICT resources. By signing this agreement you are providing consent for the school to take any action it deems necessary in order to protect community members and the School against physical or virtual threat, slander, Intellectual Property leakage, misconduct by community members and unauthorised access. The School will also take what steps it deems necessary to ensure responsible use of its information and communication technologies.
- The School has a monitoring system which enable them to review email and internet use including user details, dates viewed, times, length of time viewed, sites visited and from which computer.
- Download limits will be applied to all users and Internet content will be filtered.
- The School has intrusion detection and prevention systems that can be used to detect inappropriate activity.

SECURITY/INDIVIDUAL LOGIN

Security on the network is important. If you feel you can identify a security problem please notify the Director of ICT.

- **Under no condition should you give your password to another user.** All network violations can be traced to an individual account name and will be treated as the sole responsibility of that account holder.
- All passwords should be changed regularly.
- Do not attempt to access another person's account at any time.
- Always logout properly when using School computers. You will always be held responsible for your account activity.
- Do not deliberately engage in any activity that may cause damage to the School's ICT resources, or to anyone else's computer equipment or files.
- Misuse of a computer network is an offence under the Criminal Act.
- Any computer connected to the Collegiate SMC network must be running an antivirus utility approved by the Director of ICT.
- Files stored on the School network remain the property of the School, for which the School has legal responsibility, and reserves the right to check usage to maintain the integrity of the system.
- Any device connected to the internet only network is the responsibility of the operator to ensure it is adequately protected from virus or malicious activity the school will take no responsibility for these devices.

Exemplary Behaviour is expected at all times. When using the School's network, students 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's relationship with the School. Students will have their right to access revoked until they have restored their relationship with the School. At this point the School community will invite the student to make this commitment again.

GENERAL ICT POLICY

The School has in place an overarching ICT policy that drives the utilisation and acceptable use parameters of technology in the School. This policy also details the requirement for all Middle School Students to use a School Approved Device as part of their daily activities in the Middle School.

BYOT POLICY

This policy applies specifically to Senior School students and mandates the requirement to bring a suitable device to school on a daily basis. The BYOT program seeks to introduce more opportunity for personal preference of the type of device our Senior School students utilise, while ensuring that the devices our students bring to School are fit for purpose.



St Michael's Collegiate CyberSafety Agreement Policy 2017

Student Name: _____ School Year _____

I understand and have discussed with my parent or guardian the CyberSafety Agreement Policy for the use of Collegiate's information and communication technologies, ICT equipment /devices, network infrastructure and Internet services. I understand that I am agreeing to the policy set down by the School. I further understand that any violation of the policy is against the ethos of the School and will result in appropriate consequences and restoration.

User Signature _____

As the parent or guardian of _____, I have read the Collegiate CyberSafety Agreement Policy. I understand that the ICT equipment/devices, network and internet facilities are designed for educational purposes. I have gone through this policy with my daughter/son and understand that the misuse of these resources will result in restorative action. In agreeing to the abide by this policy I hereby give permission for my child to use Collegiate's information and communication technologies, ICT equipment /devices, network infrastructure and Internet services.

Parent's or Guardian's Name (please print) _____

Signature: _____ Date: _____