Policy & Procedure

Integrated Learning Technology Program (Secondary)

VISION AND RATIONALE

St Michael's College is committed to providing an outstanding contemporary learning environment where students and teachers are afforded the very best opportunities to develop their skills and effectively utilise available technologies to improve learning outcomes. While much has been achieved in recent years, 2020 will see this continue forward in the development of integrated learning technologies across the College. This includes:

- The further development of SEQTA, a web-based learning management system that enables teachers, students and parents/caregivers to collaborate more effectively to establish better teaching and learning opportunities.
- Secondary school students in 2020 and beyond will be issued a College-supplied device (ILT Device). This device will be handed out at their entry into the secondary campus, and a replacement device will be issued in Year 11.
- A commitment to Professional Development and technology integrated teaching and learning programs.

We are excited to be moving in a direction that will further develop rich, collaborative learning opportunities that inspire engagement and lead to improved outcomes for all.

Ownership Model

The Integrated Learning Technologies (ILT) initiative will involve the College providing technology for student use. In this model, the ILT device will be owned by the College and repairs/maintenance for the device will be arranged by the College. Distinct benefits of this arrangement include:

- Reducing costs of software licensing, including ensuring up-to-date software is installed as required;
- Ensuring a consistent platform in which to facilitate curriculum delivery;
- Enables management and support of devices;
- Enables the College to retain control over how the ILT devices are used for the lifecycle of the device in the College.

The ILT device will be issued to students at their commencement at the Secondary Campus for a 3-year life cycle. The device can used at home and outside the College.

Parents will be required to sign an Agreement with the College before the ILT device is distributed.

At the completion of Year 10 & 12 students/caregivers may have the option of taking ownership of the College supplied device. A nominal charge may be applied. If a student leaves the College before the completion These times the option to keep the device may be made available, however additional costs may apply, the amount to be determined based on departure date from the College.

As all College supplied devices are locked/secured to the St Michael's College network, they will need to be returned to IT Support to have this restriction removed so they can be used outside the e College.

So what is a "Main Device"?
Main Device refers to the main device that a Student will use during the College day to fulfil their educational requirements. In 2020 devices a College issued device will be issued to students commencing in any secondary Year.

Main Device - College Supplied
It is expected that all devices will be of a similar specification to assist in management and curriculum development. Students are not permitted to change the device specifications, make modifications or add upgrades.

Note: The manufacturer device warranty is void if attempts are made to change the hardware configuration of the device in any way. Costs for repair to the device will be the responsibility of the parent/guardian.

Specifications of the College ILT device are subject to change each year, based on current technology standards.

Students beginning at other year levels will be given a device equivalent to other students in that Year Level.

End of Lifecycle Process
The ILT device will remain the property of the College for the life of the device while the student is enrolled at the College. The device may be returned to the College at the end of the
3-year lifecycle or a buy-out option may be provided by the College. The device is expected to last for the full 3-years.

Early Return Policy
If a student leaves the College prior to the end of the ILT device's lifecycle the ILT device must be returned to the College.

The device must be in original condition as when issued and personal identifications must be removed. If the device is not returned in this condition, an additional fee will apply.

Any College issued carry case does not need to be returned.

Appearance / Personalisation
As the ILT devices are the property of the College, they are not to be altered or personalised in any way that is not completely reversible. Labels or stickers are acceptable but must be removable. Any barcode or serial number on the device should not be altered.

The protective carry case may be personalised to promote easy identification. This carry case is the property of the student and does not need to be returned (refer Early Return Policy above).

The ILT device must be carried in its carry case at all times.
If the device is not returned in its original condition or not being purchased outright, a repair cost will be incurred.

Private Devices
The use of private devices on the College's network has consequences to management and maintenance costs. The College wireless network is not able to accommodate private devices for students.

It should be noted that the College cannot support the maintenance of any private device. The College is not licensed to load software on private machines.

Longevity
Varying devices have varying build quality, this is mostly based on price. A device with cheap, flimsy hinges and plastic exterior componentry will not last as long as a better built device. A good quality device that is well looked after should easily last four years or more. However, no device can reasonably be expected to last all through high school.

Battery Life
New technology gives much longer life to modern batteries in computers. The College has purchased extra-long-life batteries for each ILT device. These should give sufficient hours of use for the College day.

The charging of devices is not permitted at the College. It is an expectation that each student will arrive at the College with their device fully charged.

Security and Storage
During the College day when the devices are not being used (e.g. at lunchtime, during PE etc.), the devices should be kept either with the student or securely stored in their locker.

The device must be properly powered off prior to storage to preserve battery life and to prevent heat build-up.

Case / Carry Bag
A strong carry case is a great way to protect your device from accidental damage. Use a bag or case designed to hold a laptop, with adequate padding.

A Carry bag is issued with all College issued ILT Devices.

Repairs and Maintenance
Students experiencing technical and software faults should:

- Back up files on a USB.
- Take the device to IT Support.

If the device is unable to be repaired by the College, it may be necessary to 're-image' the computer resulting in all files being deleted.

Be warned: a re-image process will completely reset an ILT device to original settings. PLEASE ENSURE ALL FILES ARE BACKED UP ON A USB.

Loan ILT devices are provided (if available) during repair.

During the year important updates that cannot be delivered wirelessly will require the ILT device to be returned for work to be completed. It is expected that the student may be without their ILT device for up to six days per year for servicing.

Important updates will be delivered to devices wirelessly where possible. However, devices may need to be returned to the College for servicing from time to time. Students will be informed when updates or re-imaging are required.

Damage/Loss
Any damage or loss of a College issued ILT device must be reported to IT Support as soon as possible.

Any College issued ILT device that is found by another person must be returned to IT Support as soon as possible.

Wilful or malicious damage is not covered by the manufacturer's warranty nor College policies. Repairs for damage will be charged to the parent/guardian.

Insurance
Accidental damage is covered by a College insurance policy, subject to a $100 excess. If a device is accidentally damaged parents/caregivers will be asked to pay up to a maximum of $100 to cover repair or replacement.

N.B. The insurance policy covers accidental damage only and does not cover loss or theft. If a device is stolen or lost outside the school, it may be claimable on household insurance.

No repairs on College issued devices are permitted to be performed by any third party. All repairs will be arranged/performed by St Michael's College only.

School Support
If you run into a problem, we advise students to see the IT staff. They will attempt to diagnose and provide the student with a course of action to rectify the issue.

Charging
Students should bring their device to school each day fully charged. Recharge facilities are not available in classrooms. *Students will not be permitted to recharge devices at the College.*

Software, Copyright and Intellectual Property
Software provided by the College is copyrighted and must not be distributed without written permission from the College. Students will be permitted to add their own private software if required to assist their education. All such software MUST be legally licenced by the primary user of the device and must not cause any interference with the device connecting and operating at the College. The use of any peer-to-peer sharing software (like uTorrent, Popcorn time, etc.) is not permitted. Any software loaded onto the device must not be illegal, malicious or offensive in nature and should be used in accordance with the Communications Technology Policy.

- **Antivirus**

Anti-virus software (System Centre End Point Protection) and monitoring software will be loaded onto the device through the initial imaging process. Updates of this software may be scheduled at various times.

If a student machine attempts to connect to the College network and is found to have a virus the ILT device will automatically be 'cleaned'.

Students should ensure that anti-virus software is kept up-to-date on their devices and regularly check for viruses. This can be done for no cost at the College.

As students have the right to personally use their ILT devices, and connect to the Internet from home, they need to take all steps to protect the ILT device from virus attacks.

Viruses can enter ILT devices through:
- Removable media such as USB memory sticks
- Emails
- The Internet (including web browsing, FTP programs and chat rooms)

TIPS
- *Do not open any files attached to suspicious or unknown emails.*
- *Exercise caution when downloading files from the Internet.*
- *Save the files to the ILT device's hard disk and run the virus scanner on the files before opening them.*
- *Delete chain and junk emails. Do not forward or reply to any of these.*
- *Never reply to Spam.*

Hundreds of viruses are discovered each month. Run your virus scan regularly.

- **Malware (something is better than nothing at all)**

Today malware infections are more common than virus ones. All student devices should have installed a product such as "Malwarebytes". Malware can infect all devices which can stop it from functioning correctly, steal information or lock files.

When installed, a commercially purchased Malware product will provide enhanced coverage such as real-time protection and automatic updating and scanning which will keep the device protected as much as possible.

Free alternatives are not as reliable because they require the owner to manually update the protection files and run scans manually. The device will most likely have the infection before the required update and cause the device to malfunction.

Microsoft Office (Is FREE – Do not purchase)
In our College the major piece of software teachers and students use to share learning resources and assessment is Microsoft Office. The good news is that the College makes this available via a Microsoft Licensing Agreement.

Students at the College are eligible to obtain a maximum of 5 copies of the Microsoft Office Suite to use on their home and mobile computer equipment and it remains active until you either graduate or leave the College.

Students can download this for free via their Office365 portal once they have been set up by the IT Department.

Adobe Creative Cloud
Students who are doing subjects that require Adobe Creative Suite will be able to get a copy of Adobe Creative Cloud to install. Details will be made available upon request, once required access has been verified by teaching staff.

Games & Music
The loading of this software is permitted as long as it is not used at the College and is of educational value to the student. If not, this software should not be loaded.

Headphones
The use of headphones for any sound from any device is required to reduce the interruption to other students, but must not be used for entertainment purposes whilst at the College.

Interference Issues
To protect the security of the College network and infrastructure any device found to have software that causes interference with the College network will be banned until such time as the offending software is removed and the device handed to IT Support for verification. If IT Support is satisfied that the offending software has been completely removed, this device will not be permitted to re-connect until such time as corrective action has been taken.

Internet Usage
Students can access the Internet through the College's wireless network whilst on site. Access to the Internet through the College's wireless network will be monitored and subject to strict filtering.

Students may also use the Internet for their personal use at home through their home Internet Service Provider. (Consult your ISP for processes to do this.) However, students are reminded that inappropriate downloads can be detected when the device is connected to the College's network. More information on these topics is outlined in detail in the Student Diary and the College Communications Technology Policy.

The use of any other Internet Connection technology whilst on site is strictly prohibited.

Users and Security
Each student will be required to have an individual password for logging in to the College network. This password should not be divulged to any other party under any circumstance. Sanctions will be taken against any sharing of passwords.

Any attempt to break into the College network and/or a device is a breach of the College Communications Technology Policy and penalties will apply.

The College's network logs contain information on the user logging in, the computer which is attempting to log in and various other parameters. This information can and will be used to track user access and usage. Outside access will be monitored and referred to the Police, if deemed necessary.

Internet Applications / Sites
There are significant educational benefits for some Internet applications. Some Internet sites allow its users to interact with other users. These include web-based communities, hosted services, web applications, social-networking sites, video sharing sites, wikis and blogs.

However, many of these sites can be unproductive and distracting to student learning.
The use of such web sites are based on the premise:

- The technologies and the use of the technologies do not breach any ethical and moral issues.
- The applications do not distract student learning.
- These sites are not to be accessed in class, unless specifically directed by the teacher for educational purposes.

Networks and Network Security

Ad-Hoc Networks

Ad-hoc networks (the creation of a stand-alone wireless network between two or more Devices) are strictly forbidden while at the College. The College's network security system will scan for, remove and report on any ad-hoc networks detected.

Wired Networks

Students are forbidden to plug any device into the College's wired network. Any student caught with a device plugged into the College's wired network will receive an immediate suspension of computer use. The College network security system will scan for and report on any non-College devices plugged into the College's wired network.

High Tech Crime

High Tech Crime (including Hacking) is a criminal offence. Any High Tech Crime attempts will be reported to the Police.

High Tech Crime offences are defined in Commonwealth legislation within Part 10.7 - Computer Offences of the Criminal Code Act 1995 and include, but not limited to:

- Computer intrusions (for example, malicious hacking)
- Unauthorised modification of data, including destruction of data
- Distributed denial of service (DDoS) attacks using botnets
- The creation and distribution of malicious software (for example, viruses, worms, trojans).

Packet Sniffing

Any type of software or hardware device designed to capture or view network data\packets is forbidden. Any student detected capturing network traffic will be dealt with in accordance with the College Communications Technology Policy. The College's network security system will scan for and report on any device capturing packets.

Responsible Use of Technology

If a student acts in a way that is against the contents of the College Communications Technology Policy they will be subject to consequences of the policy.

The College reserves the right to capture, store and review all internet browsing and emails across our school network.

St Michael's College maintains computers and networks so that they operate effectively to ensure the resources needed are available and that the screen interface operates in a consistent way. The following guidelines are outlined to ensure all users are able to access the latest information available, with the latest technology, in an acceptable and safe learning environment:

- Users will avoid sites with content that is violent, racist, sexist, pornographic, dominated by offensive language and/or illegal in any way.
- Engaging in chat lines or downloading files is not permitted unless forming part of a legitimate class activity guided by the teacher of that class.
- The Federal Communications Act and the St Michael's College Communications Technology Policy jointly determine guidelines for appropriate use.
- Inappropriate use of the internet and email is a serious matter and can have significant consequences, e.g. sending a message over the internet using someone else's name.
- Passwords should remain confidential. No user should log-on using another student's password.
- It is the responsibility of students to maintain sufficient credit in their printing account.
- Do not remove files or folders that have been installed to the hard disk or network.
- Do not use inappropriate or offensive names for files or folders.
- Do not bring to the College, or use, games or any other materials which may be offensive to others.
- Do not engage in cyber bulling or e-crime.
- No device (or mobile phones) with camera capabilities are to be used in change rooms or toilets.
- Under privacy legislation it is an offence to take photographs of individuals on private property without their express permission and place these images on the Internet or in the public forum.

Cyber Bullying
E-technology provides individuals with a powerful means of communicating instantly with others in both positive and negative ways.

Cyber bullying is bullying which uses e-technology as a means of victimising others. It is the use of an internet service or mobile technologies–such as email, chat room discussion groups, instant messaging, Web Pages or SMS (text messaging)–with the intention of harming another person.

Examples can include communications that seek to intimidate, control, manipulate, put down or humiliate the recipient.

Activities can include flaming (repeated negative messages), sexual and racist harassment, denigration, impersonation, trickery, exclusion and cyber stalking.

The College will investigate and take action where this kind of bullying occurs in school and outside of school having regard to the extent of harm that may have been caused to relationships between students or between students and teachers, or to the possibility that criminal behaviour may be involved.

Electronic Crime (e-crime)
Cyber bullying may involve varying levels of severity, ranging from occasional messages to frequently repeated and highly disturbing threats to a person's life.
Cyber bullying can therefore be an e-crime, a fact often not clearly understood by those involved.

E-crime occurs when a computer or other electronic communication devices (e.g. mobile phones) are used to commit an offence, are targeted in an offence, or act as a storage device in an offence.

Consequences
Any form of cyber bullying or e-crime will be dealt with through the College's "Harassment Policy" and "Acceptable Use of Information Technology Policy". Serious breaches are a Police matter and will be dealt with accordingly.

Backup and Data Storage
It is important to keep backups of critical student work. Technology can fail, be lost or stolen, so it is extremely important that all students have a backup plan in case things go wrong. There are a number of options for students to consider.

You are encouraged to use your Office 365 "OneDrive for Business Cloud Storage", and with 1TB for each student this offers ample storage. This will potentially help prevent data loss in case of computer failure or accidental user error. The OneDrive for Business Cloud Storage service also provides a recycle bin in case you want to restore deleted files if you saved them online. The College cannot be held responsible for lost work due to a failure to do backups.

Printing
Students will have access to printers on site via the 'Follow You' printing system. The use of any printer at the College will attract the same charge regardless if the printout is performed via a College desktop or student device.
To print at home, students can:
- Save work on a storage device such as a USB and use a printer-connected computer;
- Install the home printer to their device;
- Print via a wireless network card connected to a modem (refer Internet Provider for set up procedures).

Caring for your Device
Packing away your Device:
- Always store your device in the carry case and have the screen facing away from your College bag.
- Try to avoid moving your device around when it is on. Before switching it on, gently place your device on a stable surface and then switch it on.
- Be careful with the device while it is in the bag. Do not drop the bag from your shoulder. Always place the device bag down gently.
- Be careful when putting the device in the car or bus that no other items are on top of it and nothing will roll onto the device, regardless if in carry case or not.
- Devices should be switched off before being placed into the carry case.

Operating Conditions
Please do not place objects on top of your device. Avoid exposing your device to:

- Direct sunlight or sources of heat such as desk lamps.
- Dust, dirt, rain, liquids or moisture.
- Heavy shock or vibration.

LCD Screens
LCD screens are delicate – they don't like being poked, prodded, pushed or slammed. Never pick up your device by its screen. Don't slam the screen closed and always be gentle when putting your device down.

To clean your LCD screen:

- Switch off your device.
- Lightly dampen a non-abrasive cloth with water and gently wipe the screen in a circular motion.
- Do not directly apply water or cleaner to the screen.
- Avoid applying pressure to the screen.

AC Adaptor

- Connect your adaptor only to your device.
- Do not step on your power cord or place heavy objects on top of it. Keep your cord away from heavy traffic areas.
- When unplugging the power cord, pull on the plug itself, rather than the cord.
- Do not wrap THE cord too tightly around the adaptor box.
- Be aware of the power savings that come from running your device effectively from battery after being fully charged. This can be a significant amount per year.

Reminder: charging of devices at the College is prohibited.

INDEX

RELATED POLICIES, PROCEDURES AND SUPPORT DOCUMENTS

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

- Nil

REVISION RECORD

Approval Authority:	ITC Manager
Reviewed:	December 2021
Next Review Date:	December 2022