Saint Ignatius' College

Bring Your Own Device Handbook

To ensure that all children have access to unlimited opportunities to learn anytime and anywhere and that they have the tools that make this possible.

BYOD HANDBOOK 2021

Saint Ignatius' College Athelstone

Printed September 2020

HANDBOOK OVERVIEW

This document should be viewed in conjunction with the Saint Ignatius' College ICT Acceptable Use Policy.

RATIONALE

Saint Ignatius' College has a strong focus on Information and Communications Technology (ICT) literacies that will enable students to be successful global citizens in the 21st Century. ICT is a significant aspect of the College's strategic plan and the College has invested heavily to support this vision.

The Bring Your Own Device (BYOD) Model is in parallel with the strategic development of a College-wide wireless network environment.

The goal is to ensure that all students have access to unlimited opportunities to learn anytime and anywhere and that they have the tools that make this possible.

It is anticipated that a Bring Your Own Device program will result in sustainable and meaningful change to teaching and learning in our College and to prepare students for further education and training, jobs of the future and to live and work in a digital world.

In 2021 all students, Year 7 – 12, will need to have a personal laptop/device to use in the College's wireless network.

BRING YOUR OWN DEVICE (BYOD) MODEL

The College will recommend a device that we consider suitable for the type of work to be done at Year 7-12.

As many families and students already have a suitable device at home, the College will also allow parents/guardians the option for their child to bring their own device (BYOD) if it meets the minimum standards and requirements that we set in order to carry out the normal learning within the College.

VALUE AND BENEFIT OF BYOD

The establishment of the BYOD program will allow students to be efficient and organised in their daily College life. It is envisaged that individual students will be more comfortable and responsible with a personal device of choice. There will be quick and easy access to personal files, customisation of resources and provide more articulation between home and College learning connections.

We are also under no illusion that technology has the opportunity to be a distraction for many students. It can also be said that it has the potential to also act as a tool to engage them in a self-disciplined and focused manner.

The College expectation is that students act responsibly with the use of technology at all times and understand that this is a privilege that needs to be respected so they will have the opportunity to work in collaboration with their teachers and peers.

SAINT IGNATIUS' COLLEGE RECOMMENDED DEVICE

Lenovo Thinkpad L13 Yoga
A beautiful 13.3" Convertible Tablet / Ultrabook with stylus and Touch

This device will have the option to include 3 year Accidental Damage Protection Insurance *or* Accidental Damage Protection with Loss and Theft Insurance, which is strongly recommended to cover the device, as ongoing repairs to devices can prove to be very expensive. *Any device not covered by the Insurance Plan listed above would be the responsibility of the owner and their insurance company (if applicable).*

PURCHASING PORTAL

The College Purchase Portal can be accessed online at www.ignatius.sa.edu.au and then click the link under the "Shop", "Computer Device Purchase Portal". All purchases at this site will need to be **finalised by Friday 11th December 2020** to ensure that the devices will be ready for the start of the 2021 school year.

SPECIFICATIONS FOR BYOD

For those not wishing to purchase one of the "College Recommended" devices then it is acceptable for parents to source a device from their preferred vendor. If you are purchasing your own device it is vital that parents keep in mind the following features, requirements and options when selecting a device.

Battery Life: 6 hours or greater to allow for a full school day. The battery should have a full three-year warranty, or can easily have its battery changed/replaced to ensure all-day computing is still possible in the future.

Weight and portability: This needs to be appropriate for the user and also able to be carried in a school bag or laptop bag.

Screen size: Most devices are advised to be 10 – 13" and anything smaller than this can impact on eye fatigue if using the device for prolonged periods of time.

Storage. This will depend on the type of files students will be storing. Most devices come with adequate hard drive space. Cloud storage is also an option, but not all Cloud storage solutions are accessible at the College.

Memory. Most devices have a minimum of 4GB of RAM. Students wishing to use more advanced software programs should consider 8GB of RAM or greater. The iPad series would be the only exception to this rule.

Wi-Fi. Dual band capability. With many connections to the College network, less interference will be more advantageous with a 5GHz wireless option.

Some items may be considered to be additional costs and not listed in the additional pricing, such as extended warranties on battery and hardware, cordless mice, keyboards and carry case.

TECHNICAL SUPPORT

Technical support is available through the ICT Services Staff in BE207. This should be done at times when this office area is open, but not usually in lesson time. The College IT Support Staff can only troubleshoot devices they are trained to support which will be the "College Recommended" devices. For non-"College Recommended" devices, students will be asked to contact their computer supplier / manufacturer directly for all troubleshooting or repairs. **If you elect to use or buy your own device, please be aware of these important limitations:**

- The College cannot book repairs on your behalf – students will have to arrange all repairs directly with their own computer manufacturer. This may involve shipping/couriers and/or travel to service centres.
- The College cannot allocate a College loan device if required during repair procedures.
- Non-College devices will only receive very limited technical support e.g. generally only connection to College wireless system. All other troubleshooting will need to be resolved by you and your computer vendor.
- With reference to "College Recommended" devices we have a priority line to our computer vendor for repairs, with a helpdesk manager who oversees College repairs specifically. This allows us to escalate issues faster with the repair teams – due to the large amount of devices we support.
- Individual parents/students with a single laptop purchased from an independent supplier will need to use the generic manufacturer helpdesk support line which can involve lengthy phone calls.

NON-COLLEGE APPLICATIONS, GAMES AND MUSIC

Saint Ignatius' College does not object to the installation of non-College applications and files on the laptops provided that the installed applications and files:

- Are appropriately licensed (i.e. they do not breach copyright and intellectual property laws – this includes video and music downloads).
- Are ethically and morally acceptable (including consideration of College appropriateness, age appropriate ratings and privacy issues).
- Do not affect the efficient functioning of the laptops for educational purposes (i.e. they do not interfere with the speed and storage capacity of the laptop or the problems that might arise from increased battery use).
- Do not affect the College's wireless network.
- Do not interfere with the classroom learning program (i.e. they may only be used in class under specific teacher direction).

In particular, while some games have significant educational benefits and will be used under teacher direction, other games have little educational merit and may affect network function. As a result:

- The use of network games is banned (unless authorised by the teacher for educational purposes)
- Ad-hoc networks are **NOT** to be created or used.

Where there is a contravention of this policy, consequences will apply. Other sanctions may be imposed in line with the Saint Ignatius' College ICT Acceptable Use Policy.

INTERNET USAGE AT THE COLLEGE

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

Students are reminded that inappropriate download attempts can be detected when the devices are connected to the College's network. This could result in breaches to the Saint Ignatius' College ICT Acceptable Use Policy and subsequent disciplinary action.

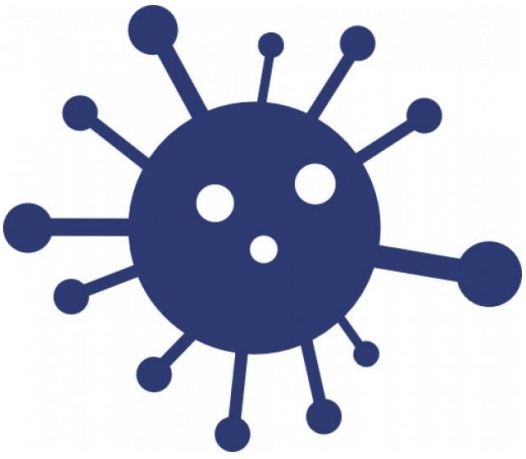
Parents need to carefully consider how they allow access to the internet at home. Wireless access can be limited through the router being turned off at times when you do not want to allow student online activity. Also cabled access in a more open home setting always allow greater information to parents about what is being accessed on the internet. If you would like further information/advice, please contact the College.

External networks such as 3G, 4G mobile networks are not permitted. All Internet access is provided by the College through password-protected wireless access points. Phone tethering, sim-related dongles and Virtual Private Networks are not to be used on College premises.

A Virtual Private Network, or VPN, is designed, amongst other things, to mask or hide internet activity. There are legitimate cases for uses of VPN's, however, most casual use of VPN's is to bypass restrictions or filters. The use of VPN's by students in our College is a breach of the "ICT Acceptable Use Policy". Internet filter systems, like those set up in our school, are used to keep students safe. Students using VPN's to bypass these restrictions, intentionally or inadvertently, are putting themselves and the College community at great risk.

Many "free" VPN services, and even some paid services, are very deceptive and dangerous. They may include inappropriate imagery in the form of advertising, or simply steal personal information, like credentials. There are significant issues with viruses or malware from the use of VPN software. These are just some of the reasons the College has always disallowed the use of VPN's.

VIRUS PROTECTION



All students must ensure that they have appropriate virus protection installed on their device. If a student machine attempts to connect to the College network and is found to have a virus the student will be notified immediately and access will be denied until the device has been cleared of any virus.

Viruses can enter laptops through removable media such as CDs, DVDs, MP3 Players, mobile phones, Bluetooth devices and USB memory sticks, emails, the Internet (including web browsing, FTP programs, online games 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 laptop'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 junk email, commonly referred to as Spam*
- *Hundreds of viruses are discovered each month. Run your virus scan regularly.*
- *If in doubt, ask **IT Support Services** for advice.*

NETWORKS AND NETWORK SECURITY

Ad-hoc Networks: Ad-hoc networks (the creation of a standalone wireless network between two or more laptops) 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. The College's network security system will scan for and report on any non-College devices plugged into the College's wired network.

Hacking: Hacking is a criminal offence under the Cyber Crime Act (2001). Police assistance will be called upon in most cases.

Packet Sniffing: Any type of software or hardware device designed to capture or view network data/packets is forbidden. The College's network security system will scan for and report any device capturing packets.

INAPPROPRIATE USE

The Manager of IT Services maintains computers and the College network so that they operate effectively, and that resources needed are available, and that College computers operate in a consistent way.

The following guidelines are outlined to ensure all users are able to access the latest research available with the latest technology in an acceptable and safe learning environment.

- Users will avoid websites 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 legitimate class activity guided by the teacher of that class.
- Inappropriate use of the internet and email is a serious matter and can have significant consequences, eg sending a message over the internet using someone else's name.
- Passwords must remain confidential. No user should log-on as another student using their password or use a computer that is logged onto the network with another students log-on.
- Do not remove files or folders that have been installed to the network.
- Do not engage in cyber-bullying or e-crime.
- Under privacy legislation it is an offence to take photographs of individuals without their expressed permission and place these images on the Internet or in the public domain.

It is a requirement of the College that any student device can only be used in designated lesson time at the direction of that subject teacher.

Devices must be stored securely in the classroom or student locker at recess and lunch breaks and are not to be used at this time unless under the direct supervision of College staff in the Campion Library.

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, Webpages 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), trolling, sexual or racist harassment, denigration, impersonation, trickery, exclusion and cyber stalking. The targeted person often feels powerless and may need help.

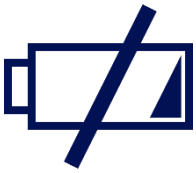
Cyber bullying may involve varying levels of severity, ranging from occasional messages to frequently repeated and highly disturbing threats to a person's life.

Consequences

Any form of cyber bullying will be dealt with through the College's 'Harassment Policy' and 'Acceptable Computer Use Policy'. Serious breaches are a police matter and may be dealt with through State and Federal Laws and SA Police.

POWER ISSUES / BATTERY / CHARGING

Charging



Students must bring the laptop to the College each day fully charged. **Students will not be permitted to recharge laptops at College. Loan batteries will not be available.**

Battery Life

New technology gives much longer life to modern batteries in computers. Students may need to adjust their power settings to ensure that their device will last the full day.

BACKUP AND DATA STORAGE

It is important for each student to keep backups of their critical work. There are a number of options students should consider.

Work can be stored on the laptop C Drive and this should be regularly backed up to a USB device or a portable USB hard drive. Work can also be stored on their H Drive on the College network. The use of Office 365 OneDrive (OneDrive for Business) is now a viable option for storing files as this gives ease of access to all stored information both on and off the campus. The College will not be held responsible for lost work due to a failure to do backups. When stored on the College network drive (the student H-Drive), work is regularly backed up.

CARING FOR YOUR LAPTOP/DEVICE

- Always store your laptop in the carry case.
- Do not wrap the cord too tightly around the power adapter or the cord will become damaged.
- Try to avoid moving your laptop around when it is on. Before switching it on, gently place your laptop on a stable surface and then switch it on.
- You still need to be careful with the laptop while it is in the bag. Do not drop the bag from your shoulder. Always place the laptop bag gently down and do not leave the laptop on the floor, even if it is in its bag.
- Be careful when putting the laptop in the car or bus that no other items are on top of it and nothing will roll on to the laptop bag.
- Laptops should be switched to at least "sleep/hibernate" mode before being placed into the bag.
- Laptops should be stored carefully in the student's locker when not in use. Students are not to leave them in an unattended or unsecured location.
- Connect your power adapter only to your laptop.
- 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 your cord too tightly around the adapter box.
- Be aware of the power savings that come from running your laptop effectively from battery, after being fully charged.

Please do not place objects on top of your laptop and never carry it around while it is turned on. Avoid exposing your laptop to:

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

Laptop and tablet screens are delicate – they don't like being poked, prodded, pushed or slammed. Never pick up your laptop by its screen. Don't slam the screen closed and always be gentle when putting your laptop down. Ensure that nothing is left on the keyboard before closing the lid. Serious, expensive damage to the screen may result if this is not done.

To clean your LCD screen:

- Switch off your laptop
- 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

STUDENT SAFETY / PARENT ADVICE

It is imperative that students are cyber safe and conduct themselves in an ethical behaviour whilst online. This should be seen as a partnership between home and the College. As children and adults spend increasing time online learning and communicating with friends we need to ensure that students are cybercitizens who know what is appropriate behaviour.

Use of a student device at home should be closely monitored by parental supervision at all times. Where possible it is highly advisable that your child's device is in your view especially when they are active on the internet / online. It is highly desirable that you do not allow your child to use their device in their bedroom and ensure that it is removed from their bedroom once they go to bed at night.

Have a personal understanding and knowledge about things like instant messaging, forums, blogs, Twitter and Facebook. As a general rule the internet is anonymous and it is not always clear who you are talking to. These personal spaces are also easily accessible to others and personal information should never be published for others to see.

Show an interest in what your child is doing on their device and online. Discuss with them the associated risks of posting or revealing personal information like their name, address, date of birth, photographs and other family information.

Explore software that allows you the parent the option to limit your child's access to inappropriate information or limit access to the internet. Most modern Wifi routers allow you to control times when specific devices that you designate can access to the internet.

Please ensure that you have adequate insurance to cover your child's device for theft or accidental damage whilst the device is used at school, as the College does not supply/cover this apart from the Insurance plan which can be purchased by parents with the device on the College Portal.

ACCESS TO THE COLLEGE WIRELESS NETWORK

Students will need to connect their device to the College wireless network. A wireless network called “IGNATIUS” is available across the College. Students will be prompted to enter their College username and password when connecting. By connecting to the College wireless network, you agree to the conditions outlined in this user guide and the ICT policies.

MICROSOFT OFFICE SOFTWARE.

Students will be licensed to use the Microsoft Office suite of programs (Office 365) – including Word, Excel, PowerPoint and One Note. New students will be able to access Office 365 at the start of Term 1 2021 in the first week of school. This license is provided by the College at no additional cost through arrangements with the Catholic Education Office and Microsoft. This copy of Office is supported on most operating systems (Windows, Apple OSX, Android, iPad iOS). Students can download Office 365 from the Microsoft Office Portal once they have received their student email address in Term 1, 2021. Students who have already received their email address may install Office from the Office 365 portal at any time.

FREQUENTLY ASKED QUESTIONS

My device is not working?	Firstly try turning it off and on again? If the problem still exists consult ICT support team for advice.
Can I print at the College?	Yes, printer access will be available through the College web printing through SEQTA. This includes all student accessible printers at the College.
Do I have to print my assignments to hand them in?	It will depend on the nature of the work and the teacher. The SEQTA Learning Management System will allow you to submit digital copies of your documents without printing.
How do I save my files?	This will depend on the type of files you will be storing. Most devices come with adequate hard drive space. Cloud storage is also an option (e.g. Office 365 OneDrive), but not all Cloud storage solutions are accessible at the College.
How do I logon to SEQTA?	Please visit https://learn.ignatius.sa.edu.au
Where do I store my device if I am in Co-curricular?	Not all co-curricular areas are safe for device storage, so the device should be kept in a safe, lockable place such as your student locker. The College offers **no responsibility** if your device is damaged or stolen during co-curricular events.
What happens if my device is damaged accidentally during College hours?	Accidents do happen and it is important to minimise this as best as possible. If you have a recommended device (*see page 3*) with damage protection/warranty, the device can be given to ICT Support and they will send it off to be replaced/repaired. If you have a device that was not purchased through the College portal, then **you** will need to seek assistance from your own supplier / insurance company.
Am I able to charge my device at the College?	No, all devices should carry enough charge to last a full school day. Please refer to **page 7** of this handbook.
Can the College look at my device?	If your device is one of the recommended devices (*see page 3*), then the College's ICT Support team will review your device when a hardware problem occurs. There is a possibility that you may receive a temporary device if further action needs to be taken. If you have a different device than the recommended, then ***only*** wireless connectivity will be checked. It will be **up to you** to contact your supplier to repair your device.
What is the name of the Saint Ignatius' College wireless network?	The name you will be looking for in your wireless list is called **Ignatius**. The other networks will not work well with all devices. The Ignatius network has been optimised for all staff and student devices.