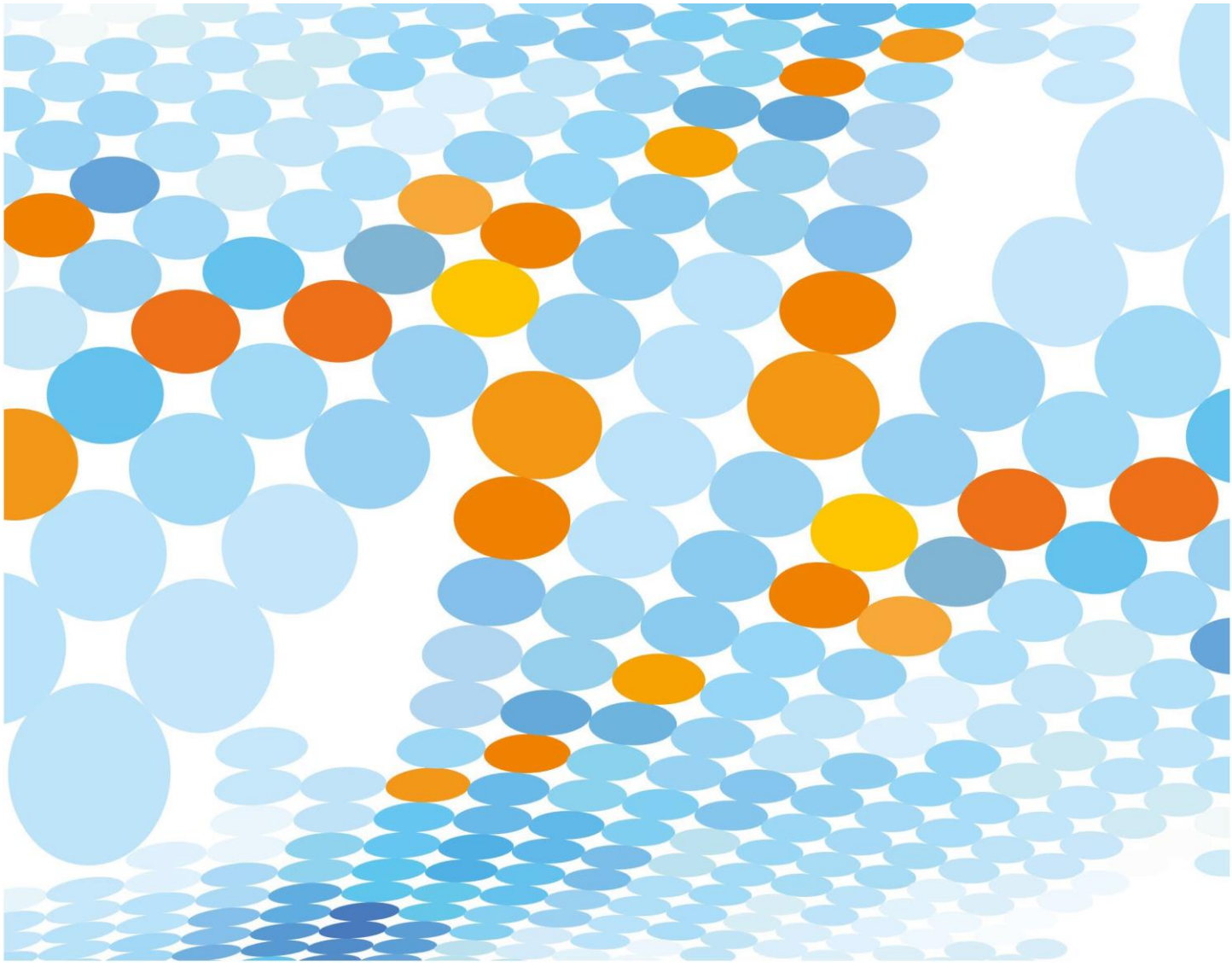
v2025

Student BYO

Laptop Charter & Agreement DOEv2025

Redlynch State College



Queensland Government

Contents

BYO Laptop Charter

BYOx overview

Bring Your Own 'x' (BYOx) is a new pathway supporting the delivery of 21st century learning. It is a term used to describe a digital device ownership model where students use their personally- owned laptop computers to access Education Queensland's information and communication (ICT) network.

The BYOx acronym refers to the teaching and learning environment in Queensland state schools, and the 'x' in BYOx represents the personal laptop with curriculum-related software applications and network connectivity.

Redlynch State College has chosen to support the implementation of a BYOx model because:

- BYOx recognises the demand for seamless movement between school, work, home and play.
- Our BYOx program assists students to improve their learning outcomes in a contemporary educational setting.
- Our BYOx program assists students to become responsible digital citizens, enhances the teaching and learning process, improves student outcomes, and imparts skills and experiences that will prepare them for their future studies and careers.

Access to Education Queensland 's ICT network is subject to the following conditions being met:

- The laptop meets or exceeds the specifications listed in "BYO Laptop selection and requirements" below.
- The laptop has an active Anti-Virus software program installed that is kept updated (see Use of mobile devices procedure.)

Students are responsible for the security, integrity, maintenance and insurance of their BYO laptops and their private network accounts.

BYO Laptop selection and requirements

Before acquiring a laptop to use at school, the parent or caregiver and student should be aware of the school's requirements concerning appropriate laptop type, technical specifications, operating system and software.

These specifications relate to the suitability of the laptop to enable class activities, meeting student needs and promoting safe and secure access to the Education Queensland's network.

For details of supported and unsupported devices and operating systems, please refer to the College BYOx webpage (https://redlynchsc.eq.edu.au/curriculum/bring-your-own-device).

The following technical specifications are required in order for a laptop to be used at Redlynch State College:

- Computer memory of 8GB RAM or more.
- Drive storage of 256GB or more.
- Minimum battery life of 6 hours to cover the school day (the charging of laptops is not allowed at school for reasons of student safety).
- Switching out of "S" mode for Windows devices is required to be able to install school curriculum-related software.
  Please refer to the document "***Switching out of S Mode in Windows***" which can be found in the "***Helpful Documents***" section on the College BYOx webpage (https://redlynchsc.eq.edu.au/curriculum/bring-your-own-device).
- The student user profile - either a local account or Microsoft account - must have Administrator privileges on the device in order to successfully enrol into Intune. Administrator privileges can be removed after the device has been successfully enrolled.
  Please refer to the document "***How to Make a User Account an Administrator in Windows"*** which can be found in the "***Helpful Documents***" section on the College BYOx webpage (https://redlynchsc.eq.edu.au/curriculum/bring-your-own-device).
- Wireless networking (5GHz Wi-Fi) - either an internal (built-in) Wi-Fi module or external USB Wi-Fi receiver.
- Only 1 (one) active anti-virus software product. All retail versions are suitable - both paid and free - including Windows Security (Microsoft Defender) which is bundled with Microsoft Windows at no additional cost.
- Microsoft 365 (Office 365).
  To obtain a free copy of Microsoft 365, please refer to the document "***Download and Install Office 365"*** which can be found in the "***Helpful Documents***" section on the College BYOx webpage (https://redlynchsc.eq.edu.au/curriculum/bring-your-own-device).

The school's BYO Laptop program **supports** printing, filtered internet access, file access and storage through the Education Queensland's network while at school.

The school's BYO Laptop program **does not** support:

- Comprehensive technical support or laptop repair.
- Charging of laptops at school.
- Security, integrity, insurance and maintenance.
- Private network accounts.

Redlynch State College ICT technicians **will provide** support to connect laptops to the school network, as well as installation of school curriculum-related software, basic technical advice and assistance to students.

Technicians **will not provide** comprehensive technical support, including but not limed to:

- Virus/malware/spyware/ransomware/etc. scanning or clean-up.
- Windows/MacOS re-installation or updates.
- Data backup and/or recovery.
- Bitlocker recovery, decryption or unlocking a device.
- Modification of Parental control software.
- Password resets or recovery for personal accounts and Apple IDs.
- Hardware repairs (e.g., screen replacement, re-seating RAM/Wi-Fi modules, etc.).

College ICT Technicians will also make available temporary storage (same-day only) and a repair space for parents or carers who have arranged for a third-party provider to repair their student's BYO laptop at school. It is the responsibility of parents or carers to arrange the repair directly with their chosen provider and to drop off & collect the laptop from the College ICT Technicians.

Additional recommendations

In addition to the requirements above, the school has the following recommendations for BYO laptops:

- Protective Case.
- Next Business Day Onsite warranty in Cairns is highly recommended.
- Accidental Damage Protection Insurance (ADP) - Check the repair timeframe, next business day if possible is recommended.
- MacBook users should be prepared to implement a dual-boot system (such as boot camp) to enable your student to be able to access Windows-based software programs. Not all curriculum-based software programs have MacOS versions.

Laptop care

The student is responsible for taking care of and securing the laptop and accessories in accordance with school policy and guidelines. Responsibility for loss or damage of a laptop at home, in transit or at school belongs to the student. Advice should be sought regarding inclusion of the laptop in your home and contents insurance policy, or taking out an Accidental Damage Protection Insurance policy for your student's laptop.

It is recommended that an extended/on-site warranty and accidental damage policy be considered at the time of purchase in order to minimise financial impact and disruption to learning should the laptop develop a fault or be damaged.

The school does not offer loan computers.

General precautions

- Food or drink should never be placed near the laptop.
- Plugs, cords and cables should be inserted and removed carefully.
- Laptops should be carried within their protective case where appropriate.
- Carrying laptops with the screen open should be avoided.
- Ensure the battery is fully charged each day.
- Turn the laptop off before placing it in its bag.
- Chargers and power banks should be visually inspected for any signs of damaged, exposed wires/parts and to manage trip hazards.
- Laptops should be visually inspected for any damaged and exposed parts.

Protecting the screen

- Avoid poking the screen - even a touch screen only requires a light touch.
- Don't place pressure on the lid of the laptop when it is closed.
- Avoid placing anything on the keyboard before closing the lid.
- Avoid placing anything in the carry case that could press against the cover.
- Only clean the screen with a clean, soft, dry cloth or an anti-static cloth.
- Don't clean the screen with a household cleaning product.

Data security and backups

Students must ensure that they regularly backup all documents on their laptops.

Student are solely responsible for backing up their laptops, and should do so to an external storage device which is kept secure (e.g., at home).

An unexpected hardware or software fault can cause all data on a laptop to be lost.

Redlynch State College is not liable for any loss of or damage to data on a student's laptop, and College ICT Technicians are not able to undertake data recovery or hardware repairs.

While at school, students are able to save data to the school's network, which is safeguarded by a scheduled backup solution. All files must be scanned using appropriate anti-virus software before being downloaded to the Education Queensland 's ICT network.

Students should also be aware that, in the event that any repairs need to be carried out the service agents may not guarantee the security or retention of the data. For example, the contents of the laptop may be deleted and the storage media reformatted.

BYOxLink – Access to digital resources between school & home

BYOxLink allows students to securely access the College's Wi-Fi network, student email and learning applications on their own laptops. It provides seamless access to digital learning resources between school and home.

In order to use BYOxLink at school, students need to enrol their laptops at home through the **Microsoft Intune Company Portal**.

Once successfully enrolled, BYO laptops will connect to the College Wi-Fi network at school and students will be able to self-install curriculum-related software.

Instructions and videos on how to enrol at home can be found in the "***Simple Steps to Connect your Device to the BYOx Network***" section on the College BYOx webpage (https://redlynchsc.eq.edu.au/curriculum/bring-your-own-device).

Acceptable laptop use

Upon enrolment in a Queensland Government school, parental or caregiver permission is sought to give the student(s) access to the internet, based upon the policy contained within the Use of ICT systems procedure.

This policy also forms part of this BYO Laptop Charter. The acceptable-use conditions apply to the use of the laptop and internet both on and off the school grounds.

Communication through internet and online communication services must also comply with the Education Queensland's Student Code of Conduct and Student Use of College Network and ICT Resources Agreement.

While on the school network, students should not:

- create, participate in or circulate content that attempts to undermine, hack into and/or bypass the hardware and/or software security mechanisms that are in place
- disable settings for virus protection, spam and/or internet filtering that have been applied as part of the school standard
- use unauthorised programs and intentionally download unauthorised software, graphics or music
- intentionally damage or disable computers, computer systems, school or government networks
- use the laptop for unauthorised commercial activities, political lobbying, online gambling or any unlawful purpose.

Note: Students' use of internet and online communication services may be audited at the request of appropriate authorities for investigative purposes surrounding inappropriate use.

Passwords

Use of the school's ICT network is secured with a username and password.

- The password must be difficult enough so as not to be guessed by other users and is to be kept private by the student and not divulged to other individuals (e.g., a student should not share their username and password with fellow students).
- The password should be changed regularly, as well as when prompted by the Education Queensland or when known by another user.
- Personal accounts are not to be shared. Students should not allow others to use their personal account for any reason.
- Students should lock or log off at the end of each session to ensure no one else can use their account or laptop.
- After successful connection to the school network, students are required to set a password or PIN to access their laptops to ensure student privacy and protection.
- Parents/caregivers may also choose to maintain a password on a laptop for access to the laptop in the event their student forgets their password or if access is required for technical support. Some laptops may support the use of parental controls with such use being the responsibility of the parent/caregiver.

Digital citizenship

Students should be conscious creators of the content and behaviours they exhibit online and take active responsibility for building a positive online reputation. They should be conscious of the way they portray themselves, and the way they treat others online.

Students should be mindful that the content and behaviours they have online are easily searchable and accessible. This content may form a permanent online record into the future.

Interactions within digital communities and environments should mirror normal interpersonal expectations and behavioural guidelines, such as when in a class or the broader community.

Parents are requested to ensure that their child understands this responsibility and expectation. The Student Code of Conduct also supports students by providing school related expectations, guidelines and consequences.

Cybersafety

If a student believes they have received a computer virus, spam (unsolicited email), or they have received a message or other online content that is inappropriate or makes them feel uncomfortable, they must inform their teacher, parent or caregiver as soon as is possible.

Students must also seek advice if another user seeks personal information, asks to be telephoned, offers gifts by email or asks to meet a student.

Students are encouraged to explore and use How to make a cyberbullying complaint to talk, report and learn about a range of cybersafety issues.

Students must never initiate or knowingly forward emails, or other online content, containing:

- a message sent to them in confidence
- a computer virus or attachment that is capable of damaging the recipients' computer
- chain letters or hoax emails
- spam (such as unsolicited advertising).
- Students must never send, post or publish:
- inappropriate or unlawful content which is offensive, abusive or discriminatory
- threats, bullying or harassment of another person
- sexually explicit or sexually suggestive content or correspondence
- false or defamatory information about a person or organisation.

Parents, caregivers and students are encouraged to read the Education Queensland's Cybersafety and Cyberbullying guide for parents and caregivers.

Web filtering

The internet has become a powerful tool for teaching and learning; however, students need to be careful and vigilant regarding some web content.

While using ICT facilities, students will at all times be required to act in line with the requirements of the Student Code of Conduct, the Student Use of College Network and ICT Resources Agreement and any specific rules of the school. To help protect students (and staff) from malicious web activity and inappropriate websites, the school operates a comprehensive web filtering system.

Any laptop connected to the internet through the school network will have filtering applied. The

filtering system provides a layer of protection to staff and students against:

- inappropriate web pages
- spyware and malware
- peer-to-peer sessions
- scams and identity theft.

This purpose-built web filtering solution takes a precautionary approach to blocking websites including those that do not disclose information about their purpose and content.

The school's filtering approach represents global best-practice in internet protection measures. Despite Education Queensland's controls to manage content on the internet, it may however still be possible to access or accidentally display illegal, dangerous or offensive information.

Teachers will always exercise their duty of care but avoiding or reducing access to harmful information also requires responsible use by the student.

Students are required to report any internet site accessed that is considered inappropriate. Any suspected security breach involving students, users from other schools, or from outside the Education Queensland network must also be reported to the school.

BYO laptops have access to home and other out-of-school internet services that may not implement any internet filtering. Parents and caregivers are encouraged to install a local filtering application on the student's laptop for when they are connected in locations other than school. Parents/caregivers are responsible for appropriate internet use by students outside the school.

Parents, caregivers and students are also encouraged to visit the website of the Australian eSafety Commissioner for resources and practical advice to help young people safely enjoy the online world.

Privacy and confidentiality

Students must not use another student or staff member's username or password to access the school network or another student's laptop, including not trespassing in another person's files, home drive, email or accessing unauthorised network drives or systems.

Additionally, students should not divulge personal information via the internet or email, to unknown entities or for reasons other than to fulfil the educational program requirements of the

school. It is important that students do not publish or disclose the email address of a staff member or student without that person's explicit permission. Students should also not reveal personal information including names, addresses, photographs, credit card details or telephone numbers of themselves or others. They should ensure that privacy and confidentiality is always maintained.

Intellectual property and copyright

Students should never plagiarise information and should observe appropriate copyright clearance, including acknowledging the original author or source of any information, images, audio, etc. used.

It is also important that the student obtain all appropriate permissions before electronically publishing other people's works or drawings. The creator or author of any material published should always be acknowledged. Material being published on the internet or intranet must have the approval of the principal or their delegate and have appropriate copyright clearance.

Copying of software, information, graphics or other data files may violate copyright laws without warning and be subject to prosecution from agencies to enforce such copyrights.

Software

Schools will require software applications to be installed on BYO laptops in order to meet the curriculum needs of particular subjects. Parents/caregivers may be required to install and support the appropriate use of the software in accordance with guidelines provided by the school. This includes the understanding that software may need to be removed from the laptop upon the cancellation of student enrolment, transfer or graduation.

Monitoring and reporting

Students should be aware that all use of internet and online communication services can be audited and traced to the account of the user.

All material on the laptop is subject to audit by authorised school staff. If at any stage there is a police request, the school may be required to provide the authorities with access to the laptop and personal holdings associated with its use.

Misuse and breaches of acceptable usage

Students should be aware that they are held responsible for their actions while using the internet and online communication services. Students will be held responsible for any breaches caused by other person(s) knowingly using their account to access internet and online communication services.

The school reserves the right to restrict/remove access of BYO laptops to the intranet, internet, email or other network facilities to ensure the integrity and security of the network and to provide a safe working and learning environment for all network users. The misuse of BYO laptops may result in disciplinary action that includes, but is not limited to, the withdrawal of access to school supplied services.

Accessing the internet through mobile hotspots or VPNs

Mobile phones and portable modems have a feature that allows the laptop's mobile/cellular network (for example 4G or 5G) to be shared as a public Wi-Fi connection.

This public Wi-Fi connection is known as a hotspot. Other laptops can then connect to the internet using this hotspot.

A VPN (Virtual Private Network) provides a private internet connection that protects some network information and traffic; hides browsing, email and messaging activities; and allows unauthorised access to some geo-blocked websites.

The use of hot-spotting and/or a VPN to connect a BYO laptop to the college network is banned at school.

Why are hot-spotting and VPNs banned at school?

The internet has a wealth of useful teaching and learning resources, but it also contains significant inappropriate content and material.

When a student connects their laptop to the school's BYOx network, a comprehensive web filtering system offers protections that reduce the risk of a student being exposed to malicious web activity and inappropriate websites.

However, when a student connects their laptop to the internet through a hotspot and/or VPN, there is no filtering available. The student may be exposed to information that is illegal, dangerous or offensive. The inappropriate content may be a risk to the student and indirectly to other students in close proximity.

The use of a hotspot and/or VPN at school will result in the student breaching the conditions of the Student BYO Laptop Charter that may result in disciplinary action.

Responsible use of BYOx

Our goal is to ensure the safe and responsible use of facilities, services and resources available to students through the provision of clear guidelines.

Responsibilities of stakeholders involved in the BYOx program

School

- BYOx program induction — including information on (but not responsible for) connection, care of laptop at school, workplace health and safety, appropriate digital citizenship and cybersafety
- network connection at school
- internet filtering (when connected via the school's computer network)
- limited technical support
- some school-supplied software (e.g., Adobe, Microsoft Office 365)
- printing facilities

Students

- participation in BYOx program induction
- acknowledgement that core purpose of laptop at school is for educational purposes
- care of laptop
- appropriate digital citizenship and online safety (for more details, visit the website of the Australian eSafety Commissioner)
- security and password protection — password must be difficult enough so as not to be guessed by other users and is to be kept private by the student and not divulged to other individuals (e.g., a student should not share their username and password with fellow students)
- maintaining a current backup of data
- charging of the laptop at home
- abiding by intellectual property and copyright laws (including software/media piracy)
- internet filtering (when not connected to the school's network)
- ensuring personal login account will not be shared with another student, and laptop will not be shared with another student for any reason
- understanding and signing the BYO Laptop Charter Agreement.

Parents and caregivers

- participation in BYOx program induction
- acknowledgement that core purpose of laptop at school is for educational purposes
- internet filtering (when not connected to the school's network)
- encourage and support appropriate digital citizenship and cybersafety with students (for more details, visit the website of the Australian eSafety Commissioner)

- required software, including sufficient anti-virus software
- protective backpack or case for the laptop
- adequate warranty and insurance of the laptop
- understanding and signing the BYO Laptop Charter Agreement.

Examples of responsible use of laptops by students

- Use laptops for:
    - engagement in class work and assignments set by teachers
    - developing appropriate 21st Century knowledge, skills and behaviours
    - authoring text, artwork, audio and visual material for publication on the Intranet or Internet for educational purposes as supervised and approved by school staff
    - conducting general research for school activities and projects
    - communicating or collaborating with other students, teachers, parents, caregivers or experts as part of assigned school work
    - accessing online references such as dictionaries, encyclopaedias, etc.
    - researching and learning through the school's eLearning environment
- Ensuring the laptop is fully charged before bringing it to school to enable continuity of learning.
- Be courteous, considerate and respectful of others when using a laptop.
- Switch off and place out of sight the laptop during classes, where these laptops are not being used in a teacher directed activity to enhance learning.
- Use the BYO laptop for private use before or after school, or during recess and lunch breaks.
- Seek teacher's approval where they wish to use a laptop under special circumstances.

Examples of irresponsible use of laptops by students

- using the laptop in an unlawful manner
- creating, participating in or circulating content that attempts to undermine, hack into and/or bypass the hardware and/or software security mechanisms that are in place
- disabling settings for virus protection, spam and/or internet filtering that have been applied as part of the school standard
- downloading (or using unauthorised software for), distributing or publishing of offensive messages or pictures
- using obscene, inflammatory, racist, discriminatory or derogatory language
- using language and/or threats of violence that may amount to bullying and/or harassment, or even stalking
- insulting, harassing or attacking others or using obscene or abusive language
- deliberately wasting printing and Internet resources

- intentionally damaging any devices, accessories, peripherals, printers or network equipment
- committing plagiarism or violate copyright laws
- using unsupervised internet chat
- sending chain letters or spam email (junk mail)
- accessing private 4G/5G networks during lesson time
- knowingly downloading viruses or any other programs capable of breaching the Education Queensland's network security
- using the laptop's camera anywhere a normal camera would be considered inappropriate, such as in change rooms or toilets
- invading someone's privacy by recording personal conversations or daily activities and/or the further distribution (e.g., forwarding, texting, uploading, Bluetooth use) of such material
- using the laptop's Wi-Fi, Bluetooth or networking functionality to cheat during exams or assessments
- take into or use laptops at exams or during class assessment unless expressly permitted by school staff.

Additional considerations

- Information sent from our school network contributes to the community perception of the school. All students using our ICT facilities are encouraged to conduct themselves as positive ambassadors for our school.
- Students using the system must not at any time attempt to access other computer systems, accounts or unauthorised network drives or files or to access other people's laptops without their permission and without them present.
- Students must not record, photograph or film any students or school personnel without the express permission of the individual/s concerned and the supervising teacher.
- Students must get permission before copying files from another user. Copying files belonging to another user without their express permission may constitute plagiarism and/or theft.
- Students need to understand copying of software, information, graphics, or other data files may violate copyright laws without warning and be subject to prosecution from agencies to enforce such copyrights.
- Parents and caregivers need to be aware that damage to laptops owned by other students or staff or school may result in significant consequences in relation to breaches of expectations and guidelines in the school's Responsible Behaviour Plan.
- The school will educate students on cyber bullying, safe internet and email practices and health and safety regarding the physical use of electronic devices. Students have a responsibility to incorporate these safe practices in their daily behaviour at school.