BYODx Charter

Contents

Personally owned mobile device charter

BYODx overview

Bring Your Own 'x' (BYODx) is a pathway supporting the delivery of 21st century learning. It is a term used to describe a digital device ownership model where students or staff use their personally-owned mobile devices to access the department's information and communication (ICT) network.

These mobile devices include both laptops and tablet devices. Access to the department's ICT network is provided only if the mobile device meets the department's security requirements which, at a minimum, requires that anti-virus software has been installed, is running and is kept updated on the device Advice for State Schools on Acceptable use of ICT Facilities and Devices (see separate document for minimum device specifications).

Students and staff are responsible for the security, integrity, insurance and maintenance of their personal mobile devices and their private network accounts.

The BYODx acronym used by the department refers to the teaching and learning environment in Queensland state schools where personally-owned mobile devices are used. The 'x' in BYODx represents more than a personally-owned mobile device; it also includes software, applications, connectivity or carriage service.

The department has carried out extensive BYODx research within Queensland state schools. The research built on and acknowledged the distance travelled in implementing 1-to-1 computer to student ratio classes across the state, and other major technology rollouts.

AVID

At Loganlea SHS, our pedagogy is founded on the **A**chievement **V**ia **I**ndividual **D**etermination model, where we explicitly teach the fundamentals of **W**riting **I**nquiry **C**ollaboration **O**rganisation and **R**eading skills. Fluency in use of information and communication technologies (ICTs) is key to WICOR and deepens our pedagogy and learning experiences. As a learning community, we recognise and embrace the importance and capacity of technology to transform teaching and learning in our school. At Loganlea State High School, we incorporate technology to enhance our thought; develop technological efficacy; strengthen our organisation and collaboration skills; differentiate for students who need support or challenge; engage our students and support our ability to inquire.

Technology innovates the processes and procedures we have in place for WICOR. BYODx values learning and teaching time, promotes flexible and fluid learning experiences and develops fluency in device use. BYODx facilitates immediate and personalised access to content and provides a medium for individualised processing of information as well as collaboration. Technology maintains cohesion in learning across multiple environments such as school, home and off-campus learning. We will encourage the use of technology as a medium to deepen our pedagogy and learning experiences for every student.

Specifications of BYODx Device

Loganlea SHS recommends that all devices used by students meet the minimum specifications below to enable suitability for curriculum-based activities. The minimum specifications provided reflect the requirements for connection to the BYODx Gateway.

Device Selection

There is a huge selection when shopping for computers. Consideration should be given to the following list. The school provides a purchase option through The School Locker. Suitable devices which adhere to the school's specifications are given on the Loganlea State High School Portal, however other options are available for devices.

- **Screen size:** As this is a tool used in the classroom, it is impractical to have a screen that is too small. Be aware that touchscreen devices all offer an on screen keyboard but this can potentially stifle the learning process by not offering enough screen space to 'think'. Minimum screen size of 9 inches is required.
- **Keyboard:** Some students prefer the improved posture and typing experience that an attached or external keyboard can offer. With the more recent trend of touchscreen devices, manufacturers are offering the user more choice than just onscreen keyboards. Keyboards can now connect via Bluetooth or can even optionally attach or detach from the device. For this reason a keyboard is recommended.
- **Portability:** The physical dimensions of the device is an important consideration as your son/daughter will need to carry the device from home to school and then from class to class during the day.
- **Battery Life/CPU:** Quite a few factors influence battery life. The type of processor (CPU) that the device runs tends to be a good indicator. The race is on at present between computer chip manufacturers to deliver chips that deliver great results with very low power output. Optimise battery life through not using it outside of class and minimising the screen brightness.
- **Connectivity:** Students will connect to the LSHS network via Wi-Fi. Access to the internet outside this is achieved via your home Wi-Fi network.
- **Storage:** In the past, laptop/pc storage relied on hard drives that used a lot of energy utilising spinning disk. The newer technology solid state drives (SSD) allow for extremely fast boot up times but at present, the size of these drives are limited and expensive. Therefore, it is recommended students purchase a 16 Gb USB for additional storage.

Other Considerations

- **Padded Carry Case:** The school recommends a separate case to the standard school bag. These are available for purchase at The School Locker.
- **Backup Solution:** This could be as simple as an external hard drive for some devices.
- **Virus Protection:** A fact of life unfortunately. Even Apple Macs are not immune to getting viruses. You will be responsible for virus protection.

- **Extended Warranty:** Many manufacturers offer an extended warranty for up to three years after the date of purchase to protect against hardware failures/defects.
- **Laptop Insurance:** Used to protect against theft, accidental damage (dropped, liquid spills, falling off the roof of moving vehicles, etc.) The school highly recommends that you review your Home and Contents Insurance policy. Other insurance options are available when purchasing the device with companies including The School Locker.
- **School Lunchtime Storage:** Students can hire a school locker for $10 a term.

Students Year 7 - 12

Laptop Hardware Requirements

Recommended Requirements	
Processor	Intel Core i5
Memory (RAM)	8GB
Battery	**10+hrs**
Screen Size	12”-15.”
Resolution	1920 x 1080 FHD
Hard Drive	256GB
Network	Wifi 6 (5Ghz 802.11ax)
Operating System*	Windows 10 or 11 Home/Pro
Minimum Requirements	
Processor	Intel Core i3 (2018+ / 8th Gen+) or latest Pentium
Memory (RAM)	4GB (not recommended for new devices – recommend upgrade to 8GB)
Battery	**10+hrs**
Screen Size	10”+
Resolution	1280 x 1024
Hard Drive	128GB
Network	Wifi 5 (5Ghz 802.11ac)
Operating System*	Windows 10 or 11 Home/Pro, Mac/iOS (not recommended - high technical skill required)

- If minimum specifications are not met, the laptop cannot connect to the school network.

iPad Hardware Requirements:

Recommended requirements	
iPad 8th Generation or newer	
Large screen	Larger than 10”
Padded carry case	
Pencil facility	
External keyboard	
Device insurance	iPads are fragile and frequently screens break
Antivirus software required	

Unsupported Devices – cannot be onboarded at Loganlea SHS	• Limited support for Apple Mac • Google Chrome Books are not compatible with the school network • Android is currently not compatible with the network • Linux is not compatible with the network

Device care

The student is responsible for taking care of and securing the device and accessories in accordance with school policy and guidelines. **Responsibility for loss or damage of a device at home, in transit or at school belongs to the student.** Advice should be sought regarding inclusion in home and contents insurance policy.

It is advised that **accidental damage and warranty policies** are discussed at point of purchase to minimise financial impact and disruption to learning should a device not be operational.

General precautions

- Food or drink should never be placed near the device.
- Plugs, cords and cables should be inserted and removed carefully.
- Devices should be carried within their protective case where appropriate.
- Carrying devices with the screen open should be avoided.
- Ensure the battery is fully charged each day.
- Turn the device off before placing it in its bag.

Protecting the screen

- Avoid poking at the screen — even a touch screen only requires a light touch.
- Don’t place pressure on the lid of the device 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.

Technical support

	Connection:	Hardware:	Software:
Parents and Caregivers	✓ (home-provided internet connection)	✓	✓
Students	✓	✓	✓
School	✓ school provided internet connection	(dependent on school-based hardware arrangements)	✓ (some school-based software arrangements)
Device vendor		✓ (see specifics of warranty on purchase)	

Data security and back-ups

Students must ensure they have a process of backing up data securely. Otherwise, should a hardware or software fault occur, assignments and the products of other class activities may be lost.

The student is responsible for the backup of all data. While at school, students may be 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 department's ICT network.

Students are also able to save data locally to their device for use away from the school network. The backup of this data is the responsibility of the student and should be backed-up on an external device, such as an external hard drive or USB drive.

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 device may be deleted and the storage media reformatted.

Acceptable personal mobile device 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 Acceptable Use of the Department's Information, Communication and Technology (ICT) Network and Systems

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

Communication through internet and online communication services must also comply with the department's Code of School Behaviour and the Code of Conduct available on the school website.

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 device 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.

The school technician will check the device to ensure that all software and media has a

Passwords

Use of the school's ICT network is secured with a user name 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 department 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 log off at the end of each session to ensure no one else can use their account or device.

Students should also set a password for access to their BYODx device and keep it private.

Parents/caregivers may also choose to maintain a password on a personally-owned device for access to the device in the event their student forgets their password or if access is required for technical support. Some devices 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 school's Code of Conduct also supports students by providing school

Cybersafety

All students are required to complete a Cyber Safety Certificate.
This can either be a school-based course or an approved online course.

Enhancing Your Digital Identity: is a course for students in Years 7-10
https://www.scootle.edu.au/ec/viewing/S8752/index.html

Cybersafety - Making positive online choices: is a course for students in Years 11 and 12
https://www.scootle.edu.au/ec/viewing/S8801/index.html

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 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 department's
https://www.qld.gov.au/education/schools/health/cybersafety/cybersafety-qss

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. At all times students, while using ICT facilities and devices, will be required to act in line with the requirements of the *Code of School Behaviour*) 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 device 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. However, despite internal departmental controls to manage content on the internet, illegal, dangerous or offensive information may be accessed or accidentally displayed. 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 Department of Education network must also be reported to the school.

The personally-owned devices have access to home and other out of school internet services and those services may not include any internet filtering. Parents and caregivers are encouraged to install a local filtering application on the student's device for when they are connected in locations other than school. Parents/caregivers are responsible for appropriate internet use by students outside the school.

Parents can provide consent for students to use various websites and services using our Online Services Consent Form.

Parents, caregivers and students are also encouraged to visit the Australian Communications and Media Authority's CyberSmart website 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 device, 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 may recommend software applications 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.

Examples of Software used on Windows PC devices at Loganlea SHS.

Different departments and courses may require:

- GIMP
- Google Chrome
- Microsoft Edge
- Mozilla Firefox
- Visual Studio Code
- VLC media player

All Queensland State School students from Prep – Year 12 can now use a free copy of the Microsoft Office 2016 Suite. The Microsoft Office 2016 Suite can be downloaded by all students to their personal devices.

Instructions for Windows and Mac devices can be downloaded using the links below: https://portal.office.com/OLS/MySoftware.aspx

Guidance for Parents and Careers

As your children increasingly make use of devices that access internet at home, it is important to consider online safety issues and gaming.

The links below are a starting point for you as you navigate managing the home environment with digital devices.

https://www.esafety.gov.au/parents/issues-and-advice/parental-controls

https://raisingchildren.net.au/teens/entertainment-technology/screen-time-healthy-screen-use/managing-screen-time-teens

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

Online Safety in Queensland State Schools (PDF, 3.8MB)

https://www.qld.gov.au/education/schools/health/cybersafety

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 device 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 device 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 personally owned mobile devices 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 personally owned mobile devices may result in disciplinary action which includes, but is not limited to, the withdrawal of access to school supplied services.

Responsible use of BYODx

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 BYODx program:

School

- network connection at school
- internet filtering (when connected via the school's computer network)
- some technical support (please consult Technical support table below)
- some school-supplied software e.g. Microsoft Office 365 …
- school representative signing of BYODx Charter Agreement.

Student

- acknowledgement that core purpose of device at school is for educational purposes
- care of device
- appropriate digital citizenship and online safety (for more details, see ACMA CyberSmart)
- 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)
- some technical support (please consult Technical support table below)

- maintaining a current back-up of data
- charging of device
- 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 device will not be shared with another student for any reason
- understanding and signing the BYODx Charter Agreement.

Parents and caregivers

- acknowledgement that core purpose of device 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, see ACMA CyberSmart)
- some technical support (please consult Technical support table below)
- required software, including sufficient anti-virus software
- protective backpack or case for the device
- adequate warranty and insurance of the device
- understanding and signing the BYODx Charter Agreement.

The following are examples of responsible use of devices by students:

- Use mobile devices 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 device is fully charged before bringing it to school to enable continuity of learning.
- Be courteous, considerate and respectful of others when using a mobile device.
- Switch off and place out of sight the mobile device during classes, where these devices are not being used in a teacher directed activity to enhance learning.
- Use the personal mobile device for private use before or after school, or during recess and lunch breaks.
- Seek teacher's approval where they wish to use a mobile device under special circumstances.

The following are examples of irresponsible use of devices by students:

- using the device 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 3G/4G networks during lesson time
- knowingly downloading viruses or any other programs capable of breaching the department's network security
- using the mobile device'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 etc.) of such material
- using the mobile device (including those with Bluetooth functionality) to cheat during exams or assessments
- take into or use mobile devices at exams or during class assessment unless expressly permitted by school staff.

In addition to this:

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 devices 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 or passwords 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 mobile devices owned by other students or staff may result in significant consequences in relation to breaches of expectations and guidelines in the school's Code of Conduct
- 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.

The school's BYODx program supports personally-owned mobile devices in terms of access to:

- internet
- file access and storage
- support to connect devices to the school network.

However, the school's BYODx program does not support personally-owned mobile devices in regard to:

- technical support
- charging of devices at school
- security, integrity, insurance and maintenance
- private network accounts.

BYODx Responsible use agreement

The following is to be read and completed by both the STUDENT and PARENT/CAREGIVER:

- I have read and understood the BYODx Charter and the school Code of Conduct
- I agree to abide by the guidelines outlined by both documents.
- I am aware that non-compliance or irresponsible behaviour, as per the intent of the BYODx Charter and the Code of Coduct, will result in consequences relative to the behaviour.
- I agree to complete a Cyber Safety Certificate.
- I am aware that my School Fees need to be paid or be on an approved Payment Plan to be able to participate.

Student's name: .....… **Year:** ..... **ID No** .....…….....….....
(Please print)

Student's signature: ......…….....…….....**Date:** / /

Parent's/caregiver's name:.....….....…….....
(Please print)

Parent's/caregiver's signature: .....…….....**Date:** / /