



Bring Your Own Device (BYOx) Student Charter Agreement

Tannum Sands State High School

Ph 07 4979 9777

Jeff Burrows

I.T. Technician

jburr76@eq.edu.au

v8 2025/26

Contents

Tannum Sands State High School	1
Student BYOx charter	1
Personally-owned mobile device charter	3
BYOx overview	3
Device selection	3
Minimum Specifications.....	4
Device care.....	5
Data security and back-ups.....	6
Acceptable personal mobile device use	7
Passwords	7
Digital citizenship.....	8
Cybersafety	8
Web filtering.....	9
Privacy and confidentiality	10
Intellectual property and copyright	10
Software	10
Monitoring and reporting	11
Misuse and breaches of acceptable usage.....	11
Responsible use of BYOx.....	11
BYOx Program includes	15
BYOx Student Laptop Charter Student-Parent Agreement (summary).....	17

Personally-owned mobile device 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 or staff use their personally-owned mobile devices to access the department's information and communication (ICT) network.

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](#).

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

The BYOx 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 BYOx represents more than a personally-owned mobile device; it also includes software, applications, connectivity or carriage service.

The department has carried out extensive BYOx 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.

We have 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
- Assisting students to become responsible digital citizens enhances the teaching learning process and achievement of student outcomes as well as the skills and experiences that will prepare them for their future studies and careers.

Device selection

Before acquiring a device to use at school, the parent or caregiver and student should be aware of the school's specification of appropriate device type, operating system requirements and software. These specifications relate to the suitability of the device to enabling class activities, meeting student needs and promoting safe and secure access to the department's network.

Please note: Up to 3 devices can be connected per student account. E.g. Laptop, iPad and Phone.

Unsupported devices – cannot connect to Education Queensland network

- Chromebook
- Android
- Linux, Unit, BSD, Raspbian
- Windows SE & Windows RT, Windows Surface 8, Windows Mobile
- Any other operating system not covered in supported devices below
- **Windows 10\11 S aka Windows 10\11 in S mode** is not supported however this can be updated to Windows Home (currently free as of 11/11/24), see guide on www.tannum.me

Laptop Minimum Specifications

- **Windows Laptop / Tablet** - Windows 10 or 11 Home or Pro
- or **Apple MacBook** - OSX 12.5.7 minimum
- Physical Keyboard
- 128Gb of Internal Storage
- 4Gb Memory
- 11" Screen
- USB Port
- 5 hours battery life
- Wi-Fi
- Under 1500g

Students with IT / Graphics classes may wish to consider a more powerful device with at least double the memory and storage, plus a bigger screen if using device at home for I.T. / Graphics home work. Decent processing power is also desired but not essential.

I.T. / Graphics students use powerful desktop computers in a lab environment while at school.

Students in grades 7-10 who are not taking IT / Graphics classes and only want to use the device for research and assignments, etc. may consider using one of the other supported devices listed below. We highly recommend one of the above devices for 11 and 12 students.

Please note: All devices will have access to the schools Internet and network drives. Windows devices will have direct access to printers (installed in control panel). MacBook laptops, iPad devices will have access to printers through a web portal.


Other supported devices

- Apple iPad, Apple iPad Mini, iPad Pro, Apple iPod Touch – Latest IOS

Supported Web Browsers

- Windows –Edge, Google Chrome
- Apple iPad / iPod Touch iOS – Safari, Edge
- Apple MacBook OSX – Safari, Google Chrome

Required Software at owners expense

- Windows – Antivirus / Internet Security application comes complete with Windows and is more than adequate. If you choose to install other applications this is at your expense and you must maintain an active subscription or remove the software to return to Windows Security
- Apple iPad / iPad Mini iOS to be installed from the app store
 -  GoodReader – PDF Edit & Viewer (also File Manager) approx. \$9.99
 - Word, Excel, PowerPoint (software required for class - \$0.00)
 - Company Portal (for connecting to school network – \$0.00)

The school's BYOx program does not support charging of devices at school. Laptop chargers should remain at home and the device should be fully charged over night before attending school each day. School Technicians are here to help with all connectivity issues and help students to install school required software. Although we are not responsible for diagnosing and fixing your faulty laptop, we will help you out wherever we can.

When students have an issue with their device, even if it seems fatal, they should bring the device to school technician so we can offer a quote for repair or replacement and offer a loan device.

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.
- Do not place other items in the case to avoid screen damage from bumps.
- Carrying devices with the screen open should be avoided.
- Ensure the battery is fully charged each day.
- Ensure the device is brought to school 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.
- Close the screen carefully ensuring there is nothing on the keyboard.

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 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 Laptop 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 Responsible Behaviour Plan 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.

While at school, **students must not connect their BYOx device to 3G/4G device or via Hot Spot** to their phone due to security and safety reasons. When use at school, students need to ensure they are connected to the EQNET network.

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 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 BYOx 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 Responsible Behaviour Plan 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 the ['Cybersafety Help button'](#) 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 department'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. 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 Queensland DET 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, 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 will 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 will need to be removed from the device upon the cancellation of student enrolment, transfer or graduation. Tannum Sands SHS offers **Microsoft Office 2019 & Adobe Creative Cloud** in the BYOx solution. Other software is available via download from the vendor. Information will be emailed home (to parent and student) once signup to the program has been finalised.

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 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 device at school, workplace health and safety, appropriate digital citizenship and cybersafety (via this charter)
- 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. Adobe, Microsoft Office 365 ...
- printing facilities
- school representative signing of BYOx Charter Agreement.

Student

- participation in BYOx program induction
- 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 BYOx Charter Agreement.

Parents and caregivers

- signup using the online form (with student present)
- 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 anti-virus software (Windows 10 includes defender antivirus which is adequate)
- protective backpack or case for the device
- adequate warranty and insurance of the device
- Understanding and electronic signing the BYOx Charter Agreement.

Technical support responsibility

	Connection:	Hardware:	Software:
Parents and Caregivers	✓ (home-provided internet connection)	✓	✓
Students	✓	✓	✓
School	✓ school provided internet connection	Will offer assistance with diagnosing fault	✓ Help offered
Device vendor		✓ (see specifics of warranty on purchase)	

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 behaviors
 - 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, encyclopedias, 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 (use of phone hot spot)

- 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 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.

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

- printing
- internet

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

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

- repairing your device (hardware or software). Technical support at school will help you wherever possible and guide parents to resolve this with the vendor.
- charging of devices at school
- security, integrity, insurance and maintenance
- private network accounts.

BYOx Program includes:

- Connectivity to network (Cisco) for Internet and Emails
- Adobe Creative Cloud Suite (Windows / Mac) if required for class
- Microsoft Office Pro 2019 also supplied (free from Education Queensland)
- Access DayMap, Readcloud, MS Teams, Qlearn, Atomi
- Connection to Impero Education Pro while at school <https://www.imperosoftware.com/education-pro/>
- Technical Support (connectivity, software guides, ask us anything type help)
- Loan laptop while laptop being repaired (up to 2 weeks)
- **Nil cost for 2025 / 2026** (student resources hire scheme must be up to date)

With **Impero**, teachers will be able to see who is and who isn't connected to the school network. What else can they do?

- Lock students' screens – so eyes on me
- Broadcast Teachers presentation, with or without locked screen – so eyes on laptop screen
- Broadcast Students work
- Save a recording of Teachers presentation
- Create and deploy quick question in real-time for instant feedback. Might be good during warm up.
- Create and deploy digital exam, that could be used as warm up, or prep for real exam. Can even be automatically marked if correct question types are used.
- Send or deploy files to student laptops, great if teacher has software such as Scratch for students to quickly install in class.
- Send and Receive large files from and to student.
- Run a website or file on all student laptops in room. Big time saver.
- Chat with students and offer assistance.
- Open Live Chat / Forum with class.
- Send a message
- Assist with basic troubleshooting in class, close Windows, shutdown, restart without touching device. Unlock, locked devices. Handy if student has forgotten password to laptop.

Other cost considerations that may be at the owner's expense

- Non warranty issues
- Replacement of lost or damaged items, laptops, charger, case, etc.
- Repair of damaged items
- Insurance excess for lost or damaged items
- Cleaning services and general maintenance
- Virus removal
- Data recovery

Always contact School I.T. Support first for advice and assistance with the above.

Students can borrow a laptop while waiting repairs (up to 2 weeks). When borrowing a laptop, if damaged while in the student's possession an up to \$150 excess will apply.

BYOx Student Laptop Charter Student-Parent Agreement

The BYOx Student Charter agreement must be read and agreed to by the parent / guardian and student.

In agreeing to the charter, I acknowledge that I,

- **Have read** this Students BYOx *charter* document, including the *Use and Care of Laptop Computer* guidelines and the school's *Internet Usage Agreement* at www.tannum.me
- **Understand** the BYOx device, power supply, battery and case is my responsibility. I will bring the device in its protective case to minimise damage. I bring the device at my own risk. Tannum SHS will not be liable for any damages or costs occurred with bringing my own laptop.
- **Have updated my home insurance policy to include the device** or have arranged an alternative policy
- **Understand that I must bring the device fully charged to school each day for class.** The device should be shut down before moving to or from school to maximise battery life, and avoid overheating.
- **Understand that the school does not allow me to use chargers at school** due to health and safety issues, unless chargers are tested and tagged and a conditional letter is given from technical support
- **Understand** my responsibilities regarding the use of the laptop and the internet. Understand that while at school the device will be accessing the Impero Education Pro Platform for class content and delivery
- **Understand** that when no longer attending Tannum Sands SHS, software offered by the school must be removed. If needed school technicians will assist you with this.
- (*Student*): Agree to keep my log-in details and **password confidential at all times**, and understand that any use attributed to my password will be attributed to me
- Acknowledge that I **understand and agree with all of the conditions** detailed in the Students BYOx Charter and will endeavour to care for the device as per the guidelines.
- Understand that if my BYOx device is damaged, or faulty, I can ask to borrow a laptop while waiting repairs (up to 2 weeks). If the loan device is damaged while in student's possession, an up to \$150 excess will apply. Please see technicians with your device before submitting to repairer.
- Understand that **failure to comply** with the Charter could result in being removed from the BYOx program.
- **Give permission for School Technicians to work on the student device without the student being present**
- Understand that **students must not connect their BYOx device to 3G/4G or via phone Hot Spot** while at school due to security and safety reasons. Student are only permitted to connect to EQNET Network.
- **Have Student Resources Hire Scheme up to date**