Student BYOx Charter

2024

Forest Lake
State High School

Contents

Personally-owned Mobile Device Charter

BYOx overview

Bring Your Own 'x' (BYOx) is a new pathway supporting the delivery of 21st century learning. BYOx 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 but are not limited to laptops, tablet devices, voice recording devices (whether or not integrated with a mobile phone or MP3 player), and communication 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.**

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.

Forest Lake State High School 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 that only devices that meet the minimum specifications will be accepted into the BYOx program.** 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.

The school's BYOx program **will support printing, filtered internet access, and file access and storage through the department's network while at school.** However, the school's BYOx program **does not include school technical support or charging of devices at school or storage facilities for student owned devices.**

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 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 Forest Lake State High School network, students will:

- Promote, engage in, or share content that enhances, strengthens, and respects the hardware and/or software security mechanisms that are in place.
- Promote, engage in, or share content that encourages the responsible exploration, research, and improvement of hardware and/or software security mechanisms that are in place.
- Use authorized programs and only download software, graphics, or music that has been legally obtained.
- Ensure the integrity of computer systems, school or government networks is maintained and used as intended.
- Use the device for authorized commercial activities, respectful engagement in political discourse, responsible online activities, and adherence to the law.

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 must 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 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 **Cybersafety and Cyberbullying guide for parents and caregivers.** Further information is available at the eSafety website - https://esafety.gov.au

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 plagiarize 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. This includes the understanding that software may need to be removed from the device 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 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 responsibilities

- 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
- 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
- printing facilities
- school representative signing of BYOx Charter Agreement.

Student responsibilities

- 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.
- completion of participation agreement and payment of annual onboarding cost

Parents and caregivers responsibilities

- purchase of BYOx device with appropriate capability.
- participation in BYOx program induction
- acknowledgement that core purpose of device at school is for educational purposes
- internet filtering (when not connected to the school's network)
- completion of participation agreement

- 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 BYOx Charter Agreement.

Technical support

	Connection:	Hardware:	Software:
Parents and Caregivers	✓ (home-provided internet connection)	✓	✓
Students	✓	✓	✓
School	✓ school provided internet connection	School will provide location for vendor on- site repairs	✓ (Office 365)
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 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, 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.

- Only use the personal mobile device for private use before or after school, or during recess and lunch breaks, when approved by Principal.
- If the device is 3G or 4G enabled, the connection **MUST** be turned off before entering classes.
- Seek teacher's approval where they wish to use a mobile device under special circumstances.

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

- Using the device in a lawful and ethical manner.
- Promote, engage in, or share content that upholds and supports the integrity and security of hardware and software systems.
- Maintain and respect settings for virus protection, spam filtering, and internet filtering as per the school's standards.
- Download and use authorized software, and distribute or publish content that is respectful and appropriate.
- Use language that is respectful, inclusive, and free from obscenity, racism, discrimination, or derogatory remarks.
- Foster a safe and supportive environment by refraining from using language or making threats that could be considered bullying, harassment, or stalking.
- Interact with others respectfully and refrain from insulting, harassing, or using abusive language.
- Use printing and internet resources responsibly, avoiding intentional waste.
- Treat devices, accessories, peripherals, printers, and network equipment with care and avoid intentional damage.
- Uphold academic integrity and respect copyright laws by avoiding plagiarism and unauthorized use of copyrighted material.
- Refrain from sending chain letters or spam email (junk mail).
- Respect the learning environment by refraining from accessing private 3G/4G networks during lesson time.
- Ensure the security of the department's network by avoiding knowingly downloading viruses or other malicious programs.
- Use the mobile device's camera responsibly and appropriately, adhering to acceptable norms regarding privacy and personal boundaries.

- Respect others' privacy by refraining from recording personal conversations or daily activities and from distributing such material (e.g., forwarding, texting, uploading, Bluetooth use, etc.).

- Use mobile devices responsibly and refrain from using them to cheat during exams or assessments.

- Adhere to school policies regarding the use of mobile devices during exams or class assessments, and only use them when 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 of Forest Lake State High School.

- Students using the system must not at any time attempt to access other computer systems, accounts or unauthorized 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 mobile 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 regard to:

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

Forest Lake SHS BYOx PARTICIPATION AGREEMENT

Bring Your Own Device (BYOx)

The following is to be read, understood and completed by both the STUDENT and the PARENT / CAREGIVER and returned to IT Support in C Block before a BYOx device will be allowed access to the school's computer network.

In signing below, we acknowledge that we:

- have purchased a device that meets the minimum specifications;
- accept all policies and guidelines as per the school's behaviour policies;
- have read and understood the BYOx Charter and the Forest Lake State High School Responsible Behaviour Plan;
- agree to abide by the guidelines outlined by both documents;
- understand my responsibilities regarding the use of the device and the Internet;
- understand that non-compliance or irresponsible behaviour, as per the intent of the BYOx Charter and the Student Code of Conduct, will result in consequences relative to the behaviour, which may include access to the school's computer network being withdrawn.

Term of Agreement – This agreement remains in place while student is enrolled at Forest Lake State High School.

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: / /