iPad Usage and Personally Owned Digital Devices Charter

Musgrave Hill State School

Personally-owned mobile device charter

Students should read through this agreement WITH THEIR PARENTS OR CARERS to ensure both parties have a clear understanding of the expectations and requirements when using a school iPad/ laptop or when bringing a personal device to school and connecting to our school network.

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

Students and staff 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. At Musgrave Hill State School we prefer students to have an Apple iPad as our chosen device. Our teachers are familiar with the devices and apps and believe that iPads offer optimum learning opportunities for students. Please see the BYOx Program Requirement list and App List for specific details.

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.

The school's BYOx program may 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.

The preferred device at Musgrave Hill State School is a 32 GB iPad Air 2 or above. Please see the BYOx Program Requirement list and App List for specific details.

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.

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.

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 2017 MHSS Acceptable Use Policy contained available on the Musgrave Hill State School Website.

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 eLearning 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 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 eLearning *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.

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.

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
- 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

- 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)
- 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.

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 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.

Musgrave Hill State School eLearning Code of Behaviour

1. When I use my mobile device I agree to:

- bring my device to school every day charged and in good working order;
- have the correct apps for learning;
- have at least 2GB free space to school work;
- regularly update software and apps;
- be the only user of the device;
- always leave my device in the locked classroom during break times;
- use it for learning purposes as directed by my teacher;
- act responsibly and not use the device to find, create or send information that might be harmful, inappropriate or hurtful to me or anyone else;
- respect others when I talk to, and work with them online, and never write or participate in online bullying;
- never download apps via the school network as it is prohibited;
- never use my phone/device to call people during the School day as it is prohibited;
- NEVER photograph or video any incidents at School, including behavioural incidents such as fights.

- only use applications/games that have an appropriate age rating and that have been approved by my teacher- the rating system is shown in the table below.

- **Table1: Age ratings for apps**

Apple Age Ratings for Apps	Accessible to
4+ years	Everyone may access these apps
9+ years	Apps will be only accessible to Years 3 and above
12+ years	Apps only accessible in Year 6
17+ years	These apps are not to be accessed by Musgrave Hill Students

- only access the school wireless network for educational purposes and never access the internet through 3/ 4G, hotspots, or other independent network connection;

2. When using my mobile device to share (via email or Goodreader, or as directed by my teacher), I will:

- act in a responsible and ethical manner,
- **NOT USE CLOUD BASED STORAGE SERVICES e.g. iCloud or Dropbox TO STORE, SEND, ACCESS OR SHARE INFORMATION, and**
- protect the privacy of others, never sharing images unless I first seek permission from the individual, or as stated below.

3. When using my device as a camera I will:

- only take photos and record sound or video when it is part of a class or lesson as directed by my teacher;
- seek permission from individuals involved **before** publishing or sending photos, recorded sound or video to anyone else or to any online space. This includes uploading materials to the Learning Place- edStudio/edAlbum, blogs or the Musgrave Hill State School Facebook Page;
- seek teacher permission before uploading any content to websites;
- protect the privacy of others and never post private information about another person, at home or at school;

I understand that if I fail to abide by the terms of this agreement I will be banned from accessing my device at school for a set period (see Table 1: Consequences of Misuse), and that my parents/carer will be notified to collect my device from School.

Table 2: Consequences of misuse of device

Misuse of device	Consequence	Action
• Using 3G, or other independent network during school hours • Using device to make calls during school hours • Using device to access social media at school • Photographing/filming- without permission • Removal of the device from the classroom without permission • Other misconduct involving digital device	**FIRST WARNING** ▪ Device confiscated, **and** ▪ **No Device Period** enforced - 2 week ban, **OR** ▪ Time frame determined by the Principal	▪ Parent/Carer to pick-up from Office, **and** ▪ Letter home
▪ **2nd Repeated misuse as stated above**	**SECOND MISUSE** ▪ Device confiscated, and ▪ No Device Period enforced – rest of Term ban, OR ▪ Time frame determined by the Principal.	▪ Parent/Carer to pick-up from Office, **and** ▪ Letter home
▪ **3rd Repeated Misuse as stated above**	**THIRD MISUSE** ▪ Device confiscated ▪ No Device Period enforced ▪ Time frame determined by the Principal	▪ Parent/Carer to pick-up from Office, **and** ▪ Letter home
▪ **Online bullying or misuse of images**	▪ Device confiscated ▪ Term ban, **or** as determined by the Principal ▪ Subject to Acceptable Use Agreement and Departmental Guidelines for bullying	▪ Parent/Carer to pick-up from Office, **and** ▪ Letter home ▪ Possible further action per the Departmental ICT Acceptable Use Agreement
▪ **Accidental damage of another person's iPad or a school iPad**	**In negotiation with the Principal:** ▪ **No Device Period** enforced - 2 week ban, **OR** ▪ Time frame determined by the Principal	▪ Parent/ Carer negotiation of repair to other person's iPad
▪ **Wilful damage of another person's iPad or a school iPad**	In the event of willful, unacceptable use of the Musgrave Hill State School network, internet or hardware one or more of the following steps may be taken: ▪ Official warning ▪ Suspension of network and/or internet privileges ▪ Banning from network and/or internet resources ▪ Appropriate consequences in accordance with the School Behaviour Plan ▪ Referral to the appropriate authorities if necessary	

Responsible use agreement

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

- I have read and understood the BYOx Charter and the school Responsible Behaviour Plan.
- 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 BYOx Charter and the Responsible Behaviour Plan, will result in consequences relative to the behaviour.

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:** / /