BYOD Charter

Springfield Lakes State School

2027

Contents

Personally owned mobile device handbook 3
BYOD overview 3
SLSS vision statement 3
Device selection 4
Device care 5
Data security and back-ups 5
Acceptable personal mobile device use 6
Passwords/ Lock Codes 7
Digital citizenship 8
Cyber Safety 8
Web filtering 9
Privacy and confidentiality 10
BYOD Link Getting your child's iPad ready for school 10
Apple IDs 11
Naming the iPad 11
Intellectual property and copyright 11
Software 12
Monitoring and reporting 12
Misuse and breaches of acceptable usage 12
Responsible use of BYOD 13

Personally Owned Mobile Device Charter

BYOD overview

Bring Your Own Device (BYOD) 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.

For the purposes of this document and all further use of the BYOD term, we will be solely referring to Apple iPads as the device. Access to the department's ICT network is provided only if the iPad 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 (see Advice for State Schools on Acceptable use of ICT Facilities and Devices.)

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

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

The department has carried out extensive BYOD 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.

SLSS ICT Vision Statement:

At Springfield Lakes State School, we are embedding technology to break down barriers to learning, empowering every student to become a responsible, digitally literate citizen.

We have chosen to support the implementation of a BYOD model because:

- Our BYOD program enhances the teaching learning process and achievement of student outcomes.
- BYOD ensures every child has access to the curriculum in ways that meet their individual needs.
- BYOD builds 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 for enabling class activities, meeting student needs and promoting safe and secure access to the department's network.

The school's BYOD program may support printing, filtered internet access, and file access and storage through the department's network while at school. However, the school's BYOD program does not include school technical support or charging of devices at school.

Apple iPad must support the newest iPadOS

Preferred iPads
iPad (11th gen.- A16) | Wi-Fi | 64gb+ | 10.9" | iPadOS 26.7.1/ iPadOS 27 *please note the 12th gen will be coming in 2027
iPad (10th gen.) | Wi-Fi | 64gb+ | 10.2" | iPadOS 26.7.1/ iPadOS 27
Accepted iPads
iPad (9th gen.) | Wi-Fi | 64gb+ | iPadOS 26.7.1/ iPadOS 27
iPad mini (6th gen. and newer) | Wi-Fi | 64gb+ | iPadOS 26.7.1/ iPadOS 27
iPad Air (4rd and newer) | Wi-Fi | 64gb+ | iPadOS 26.7.1/ iPadOS 27
iPad Pro (4th – and newer) | Wi-Fi | 64gb+ | iPadOS 26.7.1/ iPadOS 27
Apple iPad must support newest iPadOS (currently 26.7.1) but iPadOS 27 for 2027 • Please note that the iPadOS is updated annually and older devices may not support the newest version, resulting in future loss of iPad use. • Prior consultation with the school must be sought if the iPad has mobile data enabled.

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 of the device 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.
- Two hands should be placed on the device when moving from area to area.

Protecting the screen

- Avoid poking at the screen — even a touch screen only requires a light touch.
- 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.
- Keep hands on own device.

Data security and back-ups

The student is responsible for the backup of all data. While at school, students are able to save data to the school’s network using OneDrive, 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.
iCloud drive should be turned off for all school-based apps and websites as it is not supported by the school 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 iCloud drive, external hard drive or USB drive.

Students should also be aware that, if 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.

Students must ensure that they have adequate space on their device as to allow for schoolwork to be saved and school apps to be installed. Please ensure that old apps are removed, burst photo are kept to a minimum, and there is adequate space to save school documents. **Please Note- DO NOT remove Company Portal app.**

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 Device 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 (VPNs are NOT supported).
- 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.

Passwords and Lock Codes

Passwords:

Use of the school's ICT network is secured with a username and password which will be shared by the school at the start of the year or up to a week after a student's start date. The password will be set by the classroom teacher, shared with the student and family, 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 only when prompted by the department or when a problem occurs. This should be done in consultation with the class teacher.

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.

Lock Codes:

Students are encouraged to securely lock their BYOD iPad and keep it private from other students. This can either be biometrics (face ID or fingerprint ID) or using a passcode or password. **It is encouraged that the passcode be the student's username (misID) given by the teacher (eg. mdorn1), or the birth month followed by the birth year (i.e. October, 2014, passcode: 1014)**

They are required to share their lock code with the classroom teacher at the start of the year and update the teacher if the lock code changes in the event the teacher needs to access the device and/or support a forgotten lock code. 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 Student Code of Conduct also supports students by providing school related expectations, guidelines and consequences.

Cyber Safety

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. This includes both in the classroom and at home.

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.

Parents and carers can investigate Cyber Safety in QLD Schools. Students are encouraged to explore and use Cyber Safety for Primary Students and learn about a range of cyber safety 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 website of the Australian eSafety Commissioner for resources and practical advice to help young people safely enjoy the online world.

Privacy and confidentiality

Students must not use another student or staff member's username or password to access the school network or another student's 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.

Getting your child's iPad ready for school

The Department of Education supports Bring Your Own (BYO) 'D' Device solution called "BYOD Link" that enables students to use their privately owned devices to access school email, learning applications, printers and shared network drives at the school.

As part of the BYOD Link project rollout, school's wireless systems have been updated to handle access from private devices and **Microsoft Intune**; a mobile device management platform, will also be introduced **(through the Company Portal app**). Watch the video here for instructions: BYOD getting device ready for school video And the following instructions: Fact sheet for parents.

What the school administration (Intune) can see on the device	What the school administration (Intune) cannot see on the device
Your school can only see information that is relevant to the school: a. Device owner. b. Device name. c. Device model. d. Device manufacturer. e. Operating system and version eg: iOS 13 or Windows 10. f. App inventory and App names, like Microsoft Office 365. g. On student and staff's personal devices the school can only see school managed Apps. h. Device serial number and IMEI.	Your school does not monitor student's use of the device a. Cannot see your child's personal information. b. Cannot see what your child is doing on their device. c. Does not track student's locations / device location. d. Does not provide information on personally installed applications. e. Does not allow uninstalling of any applications including your child's own applications. f. Home Network cannot be seen. g. Calling and web browsing history. h. Email and text messages. i. Contacts. j. Calendars. k. Passwords. l. Pictures, including what's in the photos app or camera roll. m. Files.

Apple IDs

It is strongly advised **that a child Apple ID be set for the device**. This will allow greater parental control of the device. It also stops personal photos and documents being synced between parent and child's devices. The school does not require any information in relation to the Apple ID. This also allows the Apple Classroom app to run more effectively on the child's device.

Naming the iPad

It is strongly advised **that you use your child's name for the iPad name**. This will also help to ensure Apple Classroom has the correct name for each child. The iPad name is found in the general settings "about" tab.

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. Many of the apps that come on an iPad are used in classrooms such as the weather app, clock, calendar, measure, voice memos, notes, safari, pages, numbers, keynote and should be left on the device (not removed). 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. ***Please note it is strongly suggested that you remove the news app as a widget when setting up the iPad.** Also please be aware that **VPNs are NOT supported** by Education Queensland networks so any apps using these will need to be removed from the device. It also recommended that you remove the message app from the device as the use of this cannot be blocked or monitored by our school network.

Some apps will collect and store student data and will require parental permission to use them. This will be done through QParents online consent. Please note that DENIAL of consent will mean your child will not have access to these apps an alternatives will need to be found.

All school apps will be installed through Company Portal once the iPad is connected to the school network. We will also use apps that come with the iPad such as Pages, Numbers, Keynote, Files, Photos, Camera, Clock, Calendar, Weather, Notes, Clips, iMovie, and Safari. Please ensure the device has access to these apps.

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

Responsible use of BYOD

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 BYOD program

School

- BYOD 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, Education apps …
- use of OneDrive at school to save work and back up data
- school sets and supplies mis-id (username) and password

Student

- participation in BYOD 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, visit the website of the Australian eSafety Commissioner)
- security and password protection — password must be difficult enough so as not to be guessed by other users and is to be kept private by the student and not divulged to other individuals other than the classroom teacher (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 iPad and personal login account will not be shared with another student for any reason
- understanding and signing the Student Device Charter Agreement.
- ensuring there is adequate space on the device to save files and install apps.

Parents and caregivers

- participation in BYOD program induction - see Powerpoint and all relevant materials above.
- acknowledgement that the iPad while at school is for educational purposes
- internet filtering (when not connected to the school's network)
- encourage and support appropriate digital citizenship and cyber safety with students (for more details, visit the website of the Australian eSafety Commissioner)
- 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 witnessing Student Device Charter Agreement.
- ensuring there is adequate space on the device to save files and install apps.

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)	

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 schoolwork
  - 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.

- 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
- Use the personal mobile device for private use before or after school, or during recess and lunch breaks.
- 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.
- Not having the device charged to 100% before coming to school.
- Not allowing the device to be connected to Apple Classroom.
- Not having a numerical 4-digit passcode with the child's birth date (month, year).

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 BYOD program supports personally owned iPad in terms of access to:

- internet

- file access and storage
- support to connect devices to the school network
- charging of devices at school if needed

However, the school's BYOD program does not support personally owned mobile devices regarding:

- technical support
- charging of peripheral devices (headphones, keyboards, pens)
- security, integrity, insurance and maintenance
- private network accounts