# Student BYOD Charter

# Semester 1, 2023

# Contents

# Personal Computer Use

## FOREWORD

Our Springwood State High School team is committed to providing excellence in 21st Century Teaching and Learning within a Culture of Care. We have been trialling a BYOD program for senior students. This will enable students to demonstrate their knowledge and skills in 21st century digital learning and help develop them into effective, competent and skilled digital learners.

## BYOD overview

Bring Your Own Device (BYOD) 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 use their personally-owned computers to access the department's information and communication (ICT) network.

These mobile devices include laptops and tablet devices that can be used for word processing. 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 (see Advice for State Schools on Acceptable use of ICT Facilities and Devices).

Students and parents 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 personal computer are used. This program includes more than a personal computer, but also 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.

At Springwood State High School, the BYOD selection does not include the use of a mobile phone. Pages 4 and 5 of this charter, provides a guideline of laptop/device specifications.

# BYOD PROGRAM COST

There is no additional cost to be involved in the program.

The Student Resource Scheme levy provides:

- Access to the printer network system and print credit

- BYOD Connection Licence

- WiFi and internet access when at school

- Online textbook access

- Education Perfect

- Clickview Video Software

- Subscriptions to educational software and programs

- Technical support and troubleshooting, connection and software access

## 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.

We strongly recommend that you avoid purchasing Chromebooks as they are not suitable to be used in an Education Queensland environment due to the limitations of their Operating Systems, which clashes with network restrictions set in Education Queensland Schools.

| Component | Minimum | Recommended | High-End |
|---|---|---|---|
| Processor/CPU | Intel Celeron/Pentium or AMD 'A' Series | Intel i3 or AMD Ryzen 3 | Intel i5 or AMD Ryzen 5 |
| Memory/RAM | 8GB | 8GB | 16GB |
| Storage | 128GB SSD | 256GB SSD | 512GB SSD |
| Wireless | Supports 5GHz, 802.11ac or later | Supports 5GHz, 802.11ac or later | Supports 5GHz, 802.11ac or later |
| Screen Size/Resolution | 11"- 13", 1366x768 Resolution | 13"- 14", 1366x768 Resolution | 13"- 15", 1920x1080 HD Resolution |
| Software | Office 365 (Student Subscription included with EQ Account) | Office 365 (Student Subscription included with EQ Account)<br><br>Additional Software required for classes. | Office 365 (Student Subscription included with EQ Account)<br><br>Additional Software required for classes |
| Operating System | Windows 10 / 11 macOS 10.15 or later | Windows 10 / 11 macOS 10.15 or later | Windows 10 / 11 macOS 10.15 or later |
| Typical Cost | Below $800 | $800-$1,500 | $1,500+ |

Updated Dec 2022

## 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. Students will be given the opportunity to "check in" the device into the Innovation Hub when they have classes in an outdoor environment or during lunch breaks. Devices stored must be collected before the end of the break, prior to class starting.

*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.

- Broken or damaged charging cables should be replaced.

*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.

## 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 computer 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 Springwood State High School Student Code of Conduct available on the school website.

While on the school network, students should not:

- create, participate in or circulate content that attempts to undermine, hack into and/or bypass the hardware and/or software security mechanisms that are in place

- disable settings for virus protection, spam and/or internet filtering that have been applied as part of the school standard

- use unauthorised programs and intentionally download unauthorised software, graphics or music

- intentionally damage or disable computers, computer systems, school or government networks

- use the device for unauthorised commercial activities, political lobbying, online gambling or any unlawful purpose.

- use the device to access social media sites.

*Note: Students' use of internet and online communication services may be audited at the request of school staff 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 BYOD 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 Student Code of Conduct 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 not take photographs or recordings of any staff member or student. This will be a breach of the Privacy Act, unless directed to by a teacher during a period of instruction.

- Students must never send, post or publish:

- photographs or recordings of staff or students.

- 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 student or staff member without that person's explicit permission. Students should also not reveal personal information including names, addresses, photographs, credit card details or telephone numbers of themselves or others. They should ensure that privacy and confidentiality is always maintained.

## Intellectual property and copyright

Students should never plagiarise information and should observe appropriate copyright clearance, including acknowledging the original author or source of any information, images, audio etc. used. It is also important that the student obtain all appropriate permissions before electronically publishing other people's works or drawings. The creator or author of any material published should always be acknowledged. Material being published on the internet or intranet must have the approval of the principal or their delegate and have appropriate copyright clearance.

Copying of software, information, graphics or other data files may violate copyright laws without warning and be subject to prosecution from agencies to enforce such copyrights.

## Software

Schools may recommend software applications in order to meet the curriculum needs of particular subjects. Parents/caregivers may be required to install and support the appropriate use of the software in accordance with guidelines provided by the school. 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.**

**Students should be aware that a device is subject to confiscation by school staff, where there is the belief of misuse by the student according to this policy.**

## 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 and consequences associated with major incidents as detailed in Springwood State High Schools' Student Code of Conduct.. (Pages 14 to16 provides further information regarding appropriate usage at school).

# 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 in the BYOD program:

| School | Student | Parents and caregivers |
|---|---|---|
| BYOD program induction – including information on connection, care of device at school, workplace health and safety, network connection at school | Participation in BYOD program induction<br>Understanding and signing the BYOD Agreement | Provision of a device that meets school minimum specifications |
| Some school-supplied software licensed for BYOD devices | Acknowledgement that the core purpose of using the device at school is for educational purposes | Acknowledgement that core purpose of device at school is for educational purpose |
| Access to shared network and printing facilities (Windows only) | Care of device | Internet filtering (when not connected to the school's network) |
| Access to a safe and secure online environment | Appropriate digital citizenship and online safety | Encourage and support appropriate digital citizenship and cyber safety |
| Provision of teacher training in eLearning | Security of device and password protection | Arranging for repairs of damaged or malfunctioning hardware or non-school software, including a reload or reimage of the operating system |
| IT support for minor technical issues | Maintaining a current data back-up | Required software, including sufficient anti-virus software |
| Delivering a Digital Citizenship course to BYOD students | Charging of device overnight for use each day | Protective backpack or case for the device |
| Cyber safety presentations | Abiding by intellectual property and copyright laws | Adequate warranty and insurance of the device |
| | Internet filtering (when not connected to the school's network) | Understanding and signing the BYOD Agreement |
| | Understanding and signing the BYOD Agreement | |
| | Turn off wifi when instructed by the teacher or when not being used in class | |

*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 computers 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 computer.

- Switch off and place out of sight the computer during classes, where these devices are not being used in a teacher directed activity to enhance learning.

- Use the computer 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

- allowing other students to log onto the personal device

- creating, participating in or circulating content that attempts to undermine, hack into and/or bypass the hardware and/or software security mechanisms that are in place

- disabling settings for virus protection, spam and/or internet filtering that have been applied as part of the school standard

- downloading (or using unauthorised software for), distributing or publishing of offensive messages or pictures

- using obscene, inflammatory, racist, discriminatory or derogatory language

- using language and/or threats of violence that may amount to bullying and/or harassment, or even stalking

- insulting, harassing or attacking others or using obscene or abusive language

- deliberately wasting printing and Internet resources

- intentionally damaging any devices, accessories, peripherals, printers or network equipment

- committing plagiarism or violate copyright laws

- using unsupervised internet chat

- sending chain letters or spam email (junk mail)

- accessing private 3G/4G networks during lesson time

- knowingly downloading viruses or any other programs capable of breaching the department's network security

- using the mobile device's camera anywhere a normal camera would be considered inappropriate, such as in change rooms or toilets

- invading someone's privacy by recording personal conversations or daily activities and/or the further distribution (e.g. forwarding, texting, uploading, Bluetooth use etc.) of such material

- using the mobile device (including those with Bluetooth functionality) to cheat during exams or assessments

- take into or use mobile devices at exams or during class assessment unless expressly permitted by school staff.

**In addition to this:**

- Information sent from our school network contributes to the community perception of the school. All students using our ICT facilities are encouraged to conduct themselves as positive ambassadors for our school.

- Students using the system must not at any time attempt to access other computer systems, accounts or unauthorised network drives or files or to access other people's devices without their permission and without them present.

- Students must not record, photograph or film any students or school personnel without the express permission of the individual/s concerned and the supervising teacher.

- Students must get permission before copying files from another user. Copying files or passwords belonging to another user without their express permission may constitute plagiarism and/or theft.

- Students need to understand copying of software, information, graphics, or other data files may violate copyright laws without warning and be subject to prosecution from agencies to enforce such copyrights.

- Parents and caregivers need to be aware that damage to mobile devices owned by other students or staff may result in significant consequences in relation to breaches of expectations and guidelines in the school's Student Code of Conduct.

- The school will educate students on cyber bullying, safe internet and email practices and health and safety regarding the physical use of electronic devices. Students have a responsibility to incorporate these safe practices in their daily behaviour at school.

The school's BYOD 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 BYOD 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.

SPRINGWOOD STATE HIGH SCHOOL

# BYOD Student/Parent Agreement Form

Name:_____    Care Class:_____

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

☐ I have read and understood the BYOD Charter and Springwood State High School Student Code of Conduct available on the school website.

☐ 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 BYOD Charter and the Springwood State High School Student Code of Conduct, will result in consequences relative to the behaviour.

☐ The device my student will be bringing to school to engage in digital learning activities is:

_____

☐ I understand that it is my/my child's responsibility to care for the device and it's appropriate use.

☐ I acknowledge that the school is providing a 'Hot Desk' for school IT support and initial troubleshooting services.

Please check the box if you would like your students to be able to access their School Network (H) Drive folder from their device.  This will provide them with a backup of all their work on the school network. ☐

| | | | |
|---|---|---|---|
| **Student's name:** | _____ | **School ID No:** | _____ |
| | **(Please print)** | **Year:** | _____ |
| **Student's signature:** | _____ | **Date:** | / / |
| **Parent/Caregiver's name:** | _____ | | |
| | **(Please print)** | | |
| **Parent/Caregiver's signature:** | _____ | **Date:** | / / |
| **Principal's signature:** | _____ | **Date:** | / / |