Learning for our future

Caloundra State High School

Cricos No. 00608A

# Bring Your Own Device (BYOD)

# Student 1-to-1 Learning using ICTs

Lighting the way to broad horizons and bright futures

Caloundra State High School

March 2021

# Contents

The Department of Education, Training and Employment through its *Information Management (IM) Procedure* is collecting your personal information in accordance with the *Education General Provisions Act 2006* in order to ensure:

- appropriate usage of the school network
- appropriate usage of personal devices within the school network.

The information will only be accessed by authorised school employees to ensure compliance with its *Information Management (IM) Procedure*. Personal information collected on this form may also be disclosed to third parties where authorised or required by law. Your information will be stored securely. If you wish to access or correct any of the personal information on this form or discuss how it has been dealt with, please contact the school. If you have a concern or complaint about the way your personal information has been collected, used, stored or disclosed, please also contact the school.

**Authorisation and controls**

The principal reserves the right to restrict student access to the school's ICT facilities if access and usage requirements are not met or are breached. However restricted access will not disrupt the provision of the student's educational program.

The Department of Education, Training and Employment monitors access to and usage of their ICT network. The department may conduct security audits and scans, and restrict or deny access to the department's ICT network by any personal device, if there is any suspicion that the integrity of the network might be at risk.

# Part A: Terms and Conditions

## 1. Bring Your Own Device Policy

Teachers are constantly exploring new and innovative ways to incorporate safe and secure ICT use into the educational program.  School students, only with the approval of the principal, may be permitted limited connection of personally owned BYO devices to the department's ICT network, where this benefits the student's educational program.

The increased ownership of personal electronic devices indicated that are available to the Caloundra State High School community, has influenced the schools decision to further enhance teaching and learning through the use of  electronic devices. Having individuals accessing and using personal electronic devices responsibly for their learning is important to our school community. This policy is designed to ensure that potential issues can be clearly identified and addressed and that individuals' own devices can be effectively and safely used for optimal learning and productivity outcomes.

## 2. Benefits of Mobile Computing

### 2.1. Mobile Computing

- Mobile computing is known as "Anytime, Anywhere computing" and are part of a global initiative to enhance learning experiences for students so as to:
  - extend learning beyond the boundaries of the physical classroom.
  - promote the development of  21st Century teaching and learning
  - encourage students to become lifelong learners and develop responsible cyber adults.

### 2.2. Advantages

- Research shows this initiative to be advantageous because:
  - students who access their own computers take greater care, pride and ownership of the technological device.
  - there is a direct flow to flexible forms of schooling at anytime and anywhere.
  - it extends formal learning communities to include parents, siblings and peers.
  - it enables students to continue their work in their home environment.

## 3. BYOD Policy – Learners

- This document sets out the conditions for Bring Your Own Device (BYOD) at Caloundra State High School for learners. These devices include tablets or BYO device with the capability of connecting to the Caloundra State High School wireless internet and/or internal network for the purposes of study and work. Once connected, you will have access to:
  - the internet
  - online Learning Management System
  - textbooks and textbook management systems
  - resources such as the library portals, Recognised Training Organisations and email.

### 3.1. Acceptable BYOD Use

- It is acceptable for students while at school to use BYO devices in class for:
    - assigned class work and assignments set by teachers;
    - developing appropriate literacy, communication and information skills;
    - authoring text, artwork, audio and visual material for publication on the intranet or internet for educational purposes as supervised and approved by the school;
    - conducting general research for school activities and projects;
    - communicating or collaborating with other students, teachers, parents or experts in relation to school work;
    - accessing online references such as dictionaries or encyclopaedias;
    - researching and learning through the department's eLearning environment.
- Students with their own BYO device must ensure that they:
    - switch off and place out of sight the BYO device during classes, where these devices are not being used in a teacher directed activity;
    - use camera, video or audio functions only with the explicit direction from your teacher;
    - be courteous, considerate and respectful of others when using a BYO device;
    - use personal BYO device for private use out of class time only: before or after school, or during recess and lunch breaks;
    - not knowingly download viruses or any other programs capable of breaching the department's networks security;
    - are aware that consequences will occur if someone's privacy is invaded by recording and/or distribution of personal material;
    - are not to take into or use BYO devices at exams or during class assessment, unless instructed by teacher.
- Acknowledgment by student and parent/guardian through the signing of the following agreement that a personal device connected to the school network will be operated in a lawful, ethical and safe way.

### 3.2. Safe use and device security

- You are responsible for the maintenance and upkeep of your device. Caloundra State High School does not accept responsibility for replacing or repairing lost, stolen or damaged personal electronic devices belonging to learners.
- Personal devices should be marked clearly with your name.
- Always store your device in a protective cover and follow the manufacturer's instructions for care and maintenance.
- Do not leave your device unsupervised.
- It is strongly advised that you use a password or pin on your device to deter unauthorised use of your device. This password or pin should be kept secret.
- Keep yourself and others safe by not giving out personal details to unknown sites or individuals.
- If your device has a tracking facility such as "Find my iPhone" it is advised that this is activated to assist tracking if the device is misplaced.

### 3.3. Virus Protection

- You must have an up to date Virus Protection (if applicable) on your device:
  - Protect your devices from virus attack by keeping your operating system and antivirus software up-to-date.
  - Consider running virus scans regularly after accessing the internet or personal email.
  - Exercise due caution when downloading files from the internet.
- Please note that Windows10 (Windows Defender) & OSx has virus protection inbuilt to the operating system. Trial versions of Antivirus software may cause issues connecting to the BYO server.

### 3.4. Power supply and battery management

- You must bring your device fully charged at the beginning of the day *(access to charging facilities is limited).*
- You must bring your own power supply if you need to charge your device, as ICT or other staff will not be able to lend you recharging cables or power supplies.

### 3.5. Backup and/or recovery

- You are responsible for your own backup of critical data at all times. This may be through the use of a USB, external drive, network drives or internet-based backup option (Please note that Education Queensland blocks cloud facilities through the school Wi-Fi connection). It is important to regularly back-up important work.
- Any lost work is the student's responsibility and it is strongly advised that you take precautions to avoid this problem. ICT staff will not be responsible to try to recover lost files from a student's personal device.

### 3.6. Software and applications for learning

- You may be required to purchase and/or download and install specific software/ applications ("apps") onto your device in order to access learning materials. This will be at your own expense.
- You will need access to a relevant online Application Store (e.g. iTunes App Store, Window's Store) account associated with your device in order to download most applications.
- Software required for core curriculum work will be covered through the school Student Resource Scheme and available to be installed to your BYO device.

### 3.7. Software and application updates

- You are responsible for regularly applying updates for any software or applications ("apps") needed for the purposes of learning prior to attending scheduled classes. This may be undertaken while connected to the *Caloundra State High School's* network, provided it is outside of class time.

# Student Responsibilities

## 3.8. Responsibilities for using the school's ICT facilities and devices

- Students are expected to demonstrate safe, lawful and ethical conduct when using the school's ICT network as outlined in Caloundra State High School Student Code of Conduct.
- Students cannot use another student or staff member's username or password to access the school network.
- Students should not divulge personal information (e.g. name, parent's name, address, phone numbers), via the internet or email, to unknown entities or for reasons other than to fulfil the educational program requirements of the school.
- Students need to understand that 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.

## 3.9. Responsibilities for using a personal BYO device

- Prior to any personal device being used approval from the school is required to ensure it reflects the department's security requirements.
- Students are responsible for the security, integrity, insurance and maintenance of their personal BYO devices and their private network accounts.
- All files are to be virus free when saved to the department's network.
- Any inappropriate material or unlicensed software must be removed from personal devices before bringing the devices to school and such material is not to be shared with other students.
- Unacceptable use will lead to the device being taken to the office for storage, with its collection/return to occur at the end of the school day where the device is returned to the parent or guardian. Constant reminder on irresponsible use will result in item being held at the office for parent collection.

## 4. Rights and obligations

- The Student has the right to use their BYO Device only in accordance with this Agreement.
- The Parent/Guardian must comply with the Agreement and ensure that the Student complies with the *BYOD Rules for Students* in relation to use of their personal device at the School.
- The Parent/Guardian must also comply with their respective obligations under the *School's Student Network / Internet Access Agreement* and the *School's Internet Usage Policy*.

## 5. Period of participation

- The period of this agreement is for one Calendar year, and will be reviewed annually.
- The provision may be ended earlier, at the School's absolute discretion, if:
  - the Student is no longer enrolled with the School;
  - the Student is excluded from the School;
  - if, in the opinion of the School, the Student is not meeting the School's Student Code of Conduct and educational requirements, including absenteeism, or when attendance falls below 80% without appropriate justification;
  - the Parent/Guardian fails to comply with this Agreement or the Student Network / Internet Access Agreement and the School Internet Usage Policy; or
  - the Student fails to comply with the attached Laptop Rules for Students or the School's Student Network / Internet Access Agreement and the School's Internet Usage Policy.

## 6. Status of BYO device

- Students will be responsible for their device at all times during school hours.
- In the event of loss or damage to, or caused by, the Device it is the parent and student's responsibility and no liability from the school will be agreed to.

## 7. Connection to the internet

- At school, the School's Student Network / Internet Access Agreement and the School's Internet Usage Policy govern the carriage service and connectivity to the internet supported by Caloundra State High School's Technical Support staff. The School reminds the Parent/Guardian of their obligations under this agreement.

- The department provides a web filtering system to protect schools from malicious web activity and inappropriate websites. Students' Internet browsing on departmental owned wireless connection is filtered at school.

- No web filtering system can be 100% effective and students and/or parents should notify the school as soon as possible if an unsuitable website is accessible when using the School Network, so that the school can take appropriate action.

- If Internet access at home occurs through private internet providers and is unfiltered, it is the Parent/Guardian's responsibility to monitor student Internet usage. The School accepts no responsibility for consequences of internet access outside the school (e.g. cache files for internet browsers).

## 8. Improper use

- The Parent/Guardian must ensure that the student's personal device does not have inappropriate content or used for:
    - any illegal, pornographic, fraudulent or defamatory content;
    - bulk transmission of unsolicited electronic mail;
    - sending or causing to be sent any computer worms, viruses or rogue software;
    - menacing or harass another person (or used in a way that would be regarded by a reasonable person to be offensive);
    - transmitting any harassing, obscene, indecent, offensive, or threatening material or emails;
    - reproducing, distributing, transmitting, publishing, copying or exploiting any material that constitutes an infringement of any intellectual property rights (such as copyright) of a third party; or
    - violating any laws, such as copyright and privacy laws.

## Software

- The Student/Parent/Guardian must ensure that the software that is required for the students learning is installed to the student's device. Unauthorised software is not to be on the device. Any breach of the copyright laws the Parent/Guardian may be held liable for any damages incurred.

- Students may have additional software on their BYO device. However, only licensed software should be installed. The student must hold a valid licence for any software installed and the licence must be appropriate for installation on a personal device.

- Should the laptop require repair, it is the parent's responsibility to take the device to a reputable service provider, and have an alternative for students to use in the interim.

- The school is not responsible for restoring any programs, music, pictures or other data which may have been installed by the student. Students are responsible for backing up any work or they have installed software on the BYO device.

## 9. Virus protection

- Computer viruses, malware and malicious code have the potential to severely damage and disrupt operations within the School and the Department's networks. It may be costly to restore the network, infected hardware or software to its previous state and operability.
- These can enter laptop computers through:
  - Removable media such as USB memory sticks
  - Emails / Phishing attempts (emails linking to malicious websites)
  - The internet (including web browsing, FTP programs and chat rooms)
  - File download
  - Network file shares, such as servers and shared folders
- Students have the right to use their BYO device at school for limited personal use. If accessing the Internet this should be for curriculum related activities.
- Within the constraints of the departmentally supplied software, the Parent/Guardian must take reasonable steps to prevent malware or malicious code from infecting the laptop.

## 10. Repair and maintenance

- A manufacturer's warranty is recommended for the life of the device.
- We suggest students "personalise" their BYO device with stickers and unique cases for storage and transport. We suggest that students do not use felt pens or other markers as these tend to rub off and smudge.
- BYO devices need to be identifiable as belonging to a particular student through the use of stickers/skins, cases, key rings or name labels.

## 11. Acceptance of agreement

By completing and signing the Student Resource Scheme Participation Agreement form which is included in *Student Resource Scheme* http://ppr.det.qld.gov.au/corp/finance/services/Pages/Student-Resource-Scheme.aspx , the Parent / Guardian is acknowledging they understand and accept the Terms and Conditions of this agreement.

# Part B: Rules for Students

## 1. Appropriate Conduct

- Images or sound captured by personal technology devices on the school premises or elsewhere must not be disseminated to others, for the purpose of causing embarrassment to individuals or the School for the purpose of bullying or harassment, or where without such intent a reasonable person would conclude that such outcomes may occur.
- The School has the right to invoke appropriate disciplinary processes to deal with such conduct by a student.

## 2. Internet Service

- You must not intentionally use the Laptop or internet services to which it may be connected:
  - for any illegal, pornographic, fraudulent or defamatory purposes;
  - for bulk transmission of unsolicited electronic mail;
  - to send or cause to be sent any computer worms, viruses or other similar programs;
  - to menace or harass another person (or use in a way that would be regarded by a reasonable person to be offensive);
  - to transmit any harassing, obscene, indecent, offensive, or threatening material or emails;
  - to reproduce, distribute, transmit, publish, copy or exploit any material that constitutes an infringement of any intellectual property rights (such as copyright) of a third party; or
  - in a way that violates any laws, such as privacy laws.

## 3. Cybersafety

- If the student believes they have received a computer virus or spam (unsolicited email), or if they have received a message that is inappropriate or makes them feel uncomfortable, they must inform their teacher, parent and/or guardian as soon as is possible.
- Students are encouraged to explore and use the 'Cybersafety Help' button to talk, report and learn about a range of cybersafety issues.
- Students must 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 messages, 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 or publish:
- Unacceptable or unlawful material or remarks, including offensive, abusive or discriminatory comments.
- Threats, bullying or harassment of another person.
- Sexually explicit or sexually suggestive material or correspondence.
- False or defamatory information about a person or organisation.

## 4. Passwords

- Passwords must:
  - not be obvious or easily guessed;
  - be kept confidential,
  - be changed when prompted or when known by another user.
- Personal accounts must not 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 laptop.

## 5. Bluecoat web filtering

- An internet filtering protection solution, Bluecoat provides the department with the ability to manage the inappropriate material of the department's ICT network users.
- This covers school web browsing from the department's central servers. Third party internet access such as home internet or a council wireless hotspot from the device will not be protected by the schools filtering systems.

## 6. Privacy and confidentiality

- 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.
- The student should not reveal personal information including names, addresses, photographs, credit card details or telephone numbers of themselves or others.
- It should also be ensured that privacy and confidentiality is maintained by not disclosing or using any information in a way that is contrary to any individual's interest.

## 7. Intellectual property and copyright

- Students should never plagiarise information and shall observe appropriate copyright clearance, including acknowledging the original author or source of any information used. It is also important that the student obtain all appropriate permissions before electronically publishing other people's works.
- 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.

*Acknowledgment by student and parent/guardian through the signing of the following agreement ensures that a personal device connected to the school network will be operated in a lawful, ethical and safe way.*

# Part C: Device Specifications

Minimum recommended device specification:

| **Year 7 and 8 only** | **Web and wireless enabled device** |
|---|---|
| **Device Type:** | Microsoft Windows / Apple Mac laptop or tablet (see below) or Apple iPad |
| **Operating System:** | Windows 10 (1709), MacOS 10.13 (High Sierra), iOS/iPadOS 11 |
| **Screen Size:** | 11”-13” |

| **Years 9-12**<br>**(Middle and Senior Secondary)** | **Wireless laptop computer**<br>Minimum specifications for the device are listed below: |
|---|---|
| **Device Type:** | Microsoft Windows / Apple Mac laptop |
| **Operating System:** | Windows 10 (1709), MacOS 10.13 (High Sierra) |
| **Screen Size:** | 13” * |
| **RAM:** (year 7-9) | 4GB |
| (year 10-12) | 8GB * |
| **Storage:** | 128GB (minimum)* *(HDD, SSD or eMMc)*<br>(External Hard-drive may be beneficial for back up purposes) |
| **Battery Life:** | 6+ hours |

| *** Students studying the following subjects in year 10-12** | It is recommended that a higher specification laptop is used. |
|---|---|
| Digital Solutions, Design, Film and TV, Cert IV in IT, Cert II in IDMT or Cert II in Manufacturing | |
| **Screen Size:** | 15” screen |
| **Processor:** | i5 or i7 or equivalent processor |
| **Cache:** | 8 Mb Cache recommended for Film and TV |
| **Storage:** | 512GB Storage (HDD or SSD) |

Please note computers sold with “Win10 Home” in “S” mode need to be converted to full Windows 10 operating system, before being able to on-board to the BYOx system. Instructions for updating are located on the school website.

**Unsuitable devices include:**
Windows RT, iPad Mini, Android Devices, Chromebook, Windows machine with 64GB storage or less, Windows 7/8/8.1 OS and Linux OS devices.

For more information contact:
Mrs Virginia Schaschke
HoD Technology
(07) 5436 8444
support@caloundrashs.eq.edu.au

The school can request the BYO device be presented to show appropriate content.

Students can prepare their device to Enrol on the school network by following the relevant instructions found on our school computer and internet page

# Part D: Student Charter Agreement

The Student Caloundra SHS form must be signed and returned to the school before the device is connected to the school's network via a wireless connection.
The student and parent/caregiver must carefully read the BYO charter before signing this form. Any questions should be addressed to the school and clarification obtained before signing.
In signing below, I:

- accept all policies/guidelines as per the Student Code of Conduct.
- accept that technical support will not be provided by the school and that I am responsible for the security, integrity, insurance and maintenance of my BYO device.
- understand my responsibilities regarding the use of the device and the Internet.
- understand and agree with all of the conditions detailed in the Student BYOD Charter
- agree that I am responsible for meeting the minimum requirements listed below.
  - □ Device meets minimum specifications as recommended for year level.
  - □ Device has wireless capabilities enabled.
  - □ Specified software has been provided and installed based on course of study.
- understand that failure to comply with the Student Charter could result in the device being removed from the school's wireless network.

Device Type: ______________________ Device OS:________________________________

Student's name | Signature of student | Date | Year Level

Parent / caregiver's name | Signature of parent / caregiver | Date

Designated school representative's name | Signature of school representative | Date

This agreement is subject to change and will be distributed to students and parents via the schools webpage. Please ensure that your details are current on the school system.