CHRISTIES BEACH HIGH SCHOOL

# BRING YOUR OWN DEVICE (BYOD) POLICY

## BYOD PROGRAM

All staff and students are able to connect their own personal device to the Christies Beach High School (CBHS) wireless network. It is an expectation that devices owned by students and brought to school comply with the appropriate legal operating system and software licensing requirements.

Connection to the network will allow access the following:

- access to the schools wireless network
- limited technical support
- access to the internet
- access to printing
- access to the school's web portal – portal.cbhs.sa.edu.au

*Note: access to the school's file servers is not allowed or permitted.*

Bringing a device to school and using the school's network is a privilege and not a right, and may be revoked by the school.

## ALLOWED DEVICES

To assist in teaching and learning, staff are allowed to connect any type of device to the network. Due to behavioural concerns, students are allowed to only connect a laptop to the school's network. Any attempt to connect their mobile phone or other smart device will be prohibited.

## PRINTING

- At school, users will be able to print to a printer queue and collect their printing from a nearby printer/print release station via the PaperCut App.
- Students will receive an allocation of funds every week for printing.

*Note: students can check they have sufficient credit by logging into their PaperCut account and can request additional funds from the ICT support centre or with their teacher.*

## LIMITED TECHNICAL SUPPORT

Students who require support for connecting their account to the network are able to obtain assistance from ICT Services, however any technical or software faults should be returned to the place of purchase or a preferred repairer.

## BACKUP AND DATA STORAGE

It is the student's responsibility to ensure their data is regularly backed up. The method for backing up data is dependent on the device. Users are responsible for backing up their data to the cloud or other methods such as a portable USB or hard disk.

- School network drives will not be available for storage of student work.
- Students can submit work to teachers by email or Daymap.
- The school cannot be held responsible for lost work due to a failure to backup.

CHRISTIES BEACH HIGH SCHOOL

## GAMES

The use of games within the teaching and learning program is at the discretion of the teacher. Games must be PG rated and during school time as this will impact on battery performance negatively. It is the student's responsibility for proper battery management. In particular, while some games have significant educational benefits, other games have little educational merit and may affect network function. As a result:

- the use of network games is banned
- no ad-hoc networks are to be formed.

## INTERNET USAGE

### USAGE

Internet usage is monitored and is subject to Department for Education filtering. Inappropriate downloads can be detected when devices are connected to the school's network.

### COST

Using the internet and downloading data incurs a cost when used at school. Credit for internet usage is covered in the Materials and Services fee.

## USERS AND SECURITY

- Each student has an individual password for logging in to the school network.
- This password cannot be divulged to any other party under any circumstance. Sanctions will be taken against any sharing of passwords.
- Any attempt to break into a government computer system is a Federal offence carrying strict penalties which are also applicable to minors. Our network audit logs contain information on the user logging in, the computer they are attempting to log in with plus various other parameters. This information can, and will, be used to track user access and usage.

## VIRUS PROTECTION

- Anti-virus software must be installed onto the device.
- If a student's device attempts to connect to the school network and is found to have a virus, the laptop will be disabled.
- Students should ensure that anti-virus software is kept up-to-date on their devices and regularly check for viruses.
- As students have the right to use their own laptops and connect to the internet from home, they must take all necessary steps to protect the laptop from virus attacks.

### VIRUSES CAN ENTER LAPTOPS THROUGH:

- removable media such as CDs, DVDs and USB memory sticks
- emails
- the internet (including web browsing, FTP programs and chat rooms).

### TIPS:

- do not open any files or links attached to suspicious or unknown emails
- exercise caution when downloading files from the internet. Save the files to the laptop's hard disk and run the virus scanner on the files before opening them
- delete chain and junk emails. Do not forward or reply to any of these
- never reply to spam
- hundreds of new viruses are discovered each month. Run your virus scan regularly.

CHRISTIES BEACH HIGH SCHOOL

## WEB 2.0 APPLICATIONS

There are significant educational benefits for some Web 2.0 applications. A Web 2.0 site allows its users to interact with other users. These include web-based communities, hosted services, web applications, social-networking sites, video sharing sites, wikis and blogs.

However, many Web 2.0 applications can be unproductive and distracting to student learning. If accessed at home the school will not be liable for any consequences.

Educational Web 2.0 technologies will be used as part of a student's study in various classes. The use of Web 2.0 applications are based on the condition that:

- the technologies, and the use of the technologies, do not breach any ethical and moral issues
- the applications do not distract student learning
- the Web 2.0 technologies are not to be accessed in class, unless specifically directed by the teacher for educational purposes
- Web 2.0 technologies may be accessed at recess and lunch times.

## HACKING

Hacking is a criminal offence under the Cyber Crime Act (2001). Any hacking attempts will be forwarded to SAPOL.

## INAPPROPRIATE USE

The Network Manager maintains computers and networks so they operate effectively, that necessary resources are available, and the screen interface operates in a consistent way. The following guidelines are outlined to ensure all users are able to access the latest research available with the latest technology in an acceptable and safe learning environment:

- users will avoid sites with content that is violent, racist, sexist, pornographic, dominated by offensive language and/or illegal in any way
- engaging in chat lines or downloading files is not permitted unless forming part of a legitimate class activity guided by the teacher of that class
- the Federal Communications Act determines guidelines for appropriate use
- inappropriate use of the internet and email is a serious matter and can have significant consequences, for example sending a message over the internet using someone else's name
- passwords must remain confidential. No user should log-on as another student by using their password
- it is the responsibility of students to maintain sufficient credit in their printing accounts to allow subject-related tasks to be carried out if they choose to use the school's printers
- do not bring to school, or use at school, games or any other materials which can be offensive to others
- do not engage in cyber bulling or e-crime
- no laptop (or mobile phone) with camera capabilities are to be used in change rooms or toilets
- under privacy legislation, it is an offence to take photographs of individuals and place these images on the internet or in a public forum without their expressed permission.

## CYBER BULLYING

E-technology provides individuals with a powerful means of communicating instantly with others in both positive and negative ways. Cyber bullying is bullying which uses e-technology as a means of victimising others. It is the use of an internet service or mobile technology such as email, chat room discussion group, instant messaging, WebPage or SMS (text messaging) with the intention of harming another person.

CHRISTIES BEACH HIGH SCHOOL

Examples can include communications that seek to intimidate, control, manipulate and put down or humiliate the recipient.

Activities can include flaming (repeated negative messages), sexual and racist harassment, denigration, impersonation, trickery, exclusion and cyber stalking.

The targeted person often feels powerless and may need help.

## ELECTRONIC CRIME (E-CRIME)

Cyber bullying may involve varying levels of severity, ranging from occasional messages to frequently repeated and highly disturbing threats to a person's life.

Cyber bullying can therefore be an e-crime, a fact often not clearly understood by those involved.

E-crime occurs when a computer or other electronic communication devices (eg. mobile phones) are used to commit an offence, are targeted in an offence, or act as a storage device in an offence.

### CONSEQUENCES

Any form of cyber bullying or e-crime will be dealt with through the school's Anti-Bullying and Harassment Policy and Computers and Online Resources – Acceptable Use Policy.

Serious breaches are a police matter and will be dealt with through State and Federal laws and SAPOL.

## SECURITY AND STORAGE

During the school day when the devices are not being used (for example at lunchtime and during PE etc), the devices should be kept securely locked in the student's locker. The device must be properly powered off prior to storage to preserve battery life and to prevent heat build-up.

## POWER ISSUES/BATTERY/CHARGING

Students should come to school with their laptops fully charged as NO charging is allowed in classrooms, as per Work Health and Safety regulations.

Last modified October 2019

CHRISTIES BEACH HIGH SCHOOL

# BYOD ACCEPTABLE USE POLICY

## GUIDELINES FOR USE

Parents are expected to sign, return and agree to the Terms and Conditions of the program.

- Students and parents/caregivers must sign and return this form to CBHS to indicate commitment to responsibilities regarding to the use of their laptop.
- The laptop and/or device must be charged and available for use at school each day.
- Access to the network will only be granted once this form has been returned to ICT Services.
- Access to the network will be disabled for any reason as deemed appropriate by the ICT Management Committee.

Student use of school computers and the internet must be in accordance with the school and the Department for Education acceptable use policies.

I understand and accept the responsibilities outlined in this document. This agreement will remain valid and in place for the duration of my child's enrolment at CBHS.

## PLEASE RETURN THIS FORM TO ICT SERVICES

Student Name:_____

Student Signature:_____

Parent/Caregiver Name: _____

Parent/Caregiver Signature: _____

Date: _____