CAVENDISH ROAD *State High School*

Student BYOD Charter Agreement

Years 7 – 12
Bring Your Own Device Program

CAVENDISH ROAD *State High School*

Contents

BYOD overview 3

Device selection and specifications 3

Device care and Damage/Loss 3

Data security and back-ups 4

Acceptable personal device use 4

Passwords 4

Web filtering 5

Privacy and confidentiality 5

Intellectual property and copyright 6

Software 6

Monitoring and reporting 6

Misuse and breaches of acceptable usage 6

Responsible use of BYOD 7

Website Risk Review 8

Responsible use agreement 9

CAVENDISH ROAD *State High School*

BYOD Overview

Bring Your Own device (BYOD) is being offered at Cavendish Road State High School as a new pathway supporting the delivery of 21st century learning. It is a term used to describe a personally owned device that meets Cavendish Road State High School's minimum specifications and can be connected to the Queensland Department of Education information and communication (ICT) network for teaching and learning.

Device Selection and Specifications

Cavendish Road State High has specifications for BYOD devices that are consistent with meeting curriculum needs for students of the school.

- For Years 7 – 9, the BYOD is an Apple iPad
- For Years 10 – 12, student/parent choice. Students are able to continue the use of an iPad or move to windows or apple laptop.

Before acquiring a device to use at school the parent or caregiver and student should carefully read the minimum specifications on the BYOD page on the school website. These specifications relate to the suitability of the device to enable class activities, meeting student needs and promoting safe and secure access to the department's network.

Device Connectivity and Access while at School

The school's BYOD program supports access to printing, filtered internet access, and file access and storage through the department's network while at school.

Device Technical Support

The school provides technical support limited to enabling the device to access the school network and software.

Physical damage, faulty hardware and operating system software, or removal of non- school software that prevents the device from accessing the school network are the responsibility of the student and parent/guardian.

Device Care and Damage/Loss

The student is responsible for taking care of and securing the device. Responsibility for loss or damage of a device at home, in transit and at school belongs to the student and parent. Independent advice should be sought regarding inclusion in home and contents insurance policy or separate insurance for the device. The school takes no responsibility for damage or loss.

It is advised that accidental damage and warranty policies are discussed at point of purchase to minimise financial impact and disruption to learning should a device not be operational.

Data Security and Back-ups

Students must ensure they have a process of backing up data securely. Otherwise, should a hardware or software fault occur, assignments and the products of other class activities may be lost. The student is responsible for the backup of all data. All students are required to backup work to OneDrive. Students are also able to save data locally to their device for use away from the school network, though is not recommended due to storage concerns.

Acceptable Personal device Use

Upon enrolment in a Queensland Government school, parental or caregiver permission is sought to give the student access to the internet. Communication through internet and online communication services must also comply with the *Student Code of Conduct* available on the school website, and the Student BYOD Charter Agreement.

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 will need to be changed when prompted by the department or when known by another user.

CAVENDISH ROAD *State High School*

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. To help protect students (and staff) from malicious web activity and inappropriate websites, the Queensland Department of Education 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 filtering approach applied by DOE represents global best-practice in internet protection measures. However, despite internal departmental controls to filter content on the internet, illegal, dangerous or offensive information may be accessed or accidentally displayed on the screen. Teachers will always exercise their duty of care, but avoiding or reducing access to harmful information also requires responsible use by the student.

Students must comply with the provisions of Cavendish Road State High School's *Information Communication Technology Acceptable Use Policy and Agreement* as stated in the 2022 Student Study Planner.

Privacy and Confidentiality

Students must not use another student's 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, OneDrive, 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.

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

Cavendish Road State High School may recommend software applications 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 completion of their studies at school.

Students must 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 review by authorised school staff.

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.

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 another person 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 and or device to the school supplied services.

CAVENDISH ROAD *State High School*

Responsible use of BYOD

Responsibilities of stakeholders involved in the BYOD program:

School

- BYOD program induction — including information on connection, care of device at school, workplace health and safety, network connection at school
- Some school-supplied software e.g., Adobe, Microsoft Office 365
- Access to shared network and printing facilities (Mac, iPad and Windows)
- Principal signature on BYOD Charter Agreement

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
- Security of device and password protection
- Maintaining a current back-up of data
- Charging of device fully overnight for use each day
- Abiding by intellectual property and copyright laws
- Internet filtering (when not connected to the school's network)
- Understanding and signing the BYOD device Charter Agreement

Parents and Caregivers

- Provision of a device that meets school minimum specifications
- Acknowledgement that core purpose of device at school is for educational purposes
- Internet filtering (when not connected to the school's network)
- Encourage and support appropriate digital citizenship and cyber safety
- Arranging for repair of damage or malfunctioning hardware or non-school software, including a reload or reimage of the operating system
- Required software, including sufficient anti-virus software
- Protective backpack or case for the device
- Adequate warranty and insurance of the device
- Understanding and signing the BYOD device Charter Agreement