MARRYATVILLE HIGH SCHOOL

BRING YOUR OWN DEVICE (BYOD)

STUDENT & PARENT BOOKLET

Year 11 & 12 Students only

YEAR 11 & 12 Bring Your Own Device (BYOD)

Dear Parent / Caregiver,

Marryatville High School has a Laptop Program which requires students to purchase a prescribed laptop on entry to the school. A range of curriculum & pedagogy implications require students to maintain these devices for the duration of Year 8 – 10 (this period is also covered by manufacturer's warranty). We are however aware, that by Year 11 and 12, these devices may no longer be at peak function and some families choose to purchase replacement devices which are non-school specified.

Our recent ICT upgrades have now positioned us ready to adopt a BYOD scheme for senior students. We would like to offer Year 11 & 12 students with non-school devices (that meet prescribed minimum standards) opportunity to connect to the internet at school.

The following documents outline a range of 'conditions for use' and should be read carefully.

- Student expectations
- Supervision and monitoring
- Software installation
- Virus protection
- Networks and security
- Damage
- Charging
- Cancellation of connection
- Required and recommended device specifications
- Access & technical support

To take up the BYOD opportunity students and families must undertake the following steps:

1. **Read the enclosed documentation**
    a. BYOD Policy
    b. BYOD Guidelines

2. **Determine whether your device meets minimum recommended standards**

3. **Read and sign the following documents:**
    a. Cyber Safety Use Agreement
    b. BYOD Declaration

4. **Make a BYOD appointment with the IT Help Desk via our online booking system**
    a. Appointments can be made via the BYOD tab on the school website
        i. Year 12 students can make appointments from 24.5.17
        ii. Year 11 students can make appointments from 31.5.17
    b. Login details: Student SURNAME Password : Student ID
    c. If students miss scheduled appointment times they will need to rebook

5. **Attend a scheduled Help Desk appointment to finalise the BYOD connection. The process will take approximately 10 minutes:**
    a. Student device specifications will be checked and validated
    b. Provide signed Cyber Safety & BYOD Declaration forms
    c. Instructions for 'self on-boarding' will be provided.

Please note whilst every effort will be made to accommodate student applications for the BYOD option, some technical issues may prevent some devices from connecting.

Yours sincerely
Julie Ferguson
Acting Principal

Marryatville High School BYOD Policy

Aim/Purpose
As a school we continue to focus on the use of digital technologies to enhance our teaching and learning environments. This involves the development and use of 'virtual' or 'flexible' learning environments, which extend the classroom experience beyond the physical space of school. We need to ensure that all students have compatible devices that align with the schools infrastructure and facilitate productive learning and teaching.

Rationale
Every student has access to a personal device in order to foster the seamless integration of digital technologies into the teaching and learning environments of the school.
- Year 8 – 10 students are required to purchase or borrow a school specified device
- Year 11 & 12 students may use a school specified device or bring their own device (BYOD)

Definition
Bring your own device (BYOD) refers to a technology model where students bring a personally owned device to school for the purpose of learning. A personally owned device is any technology device brought into the school and owned by a student (or the student's family), staff or guests. Devices suitable for use at Marryatville High School are further defined in the Guidelines and User Agreement.

Responsibilities
Staff
- Support and encourage safe and ethical use of BYOD in their classes
- Model appropriate and ethical use of ICT Devices
- Report suspected student violations of school policies, administrative procedures, school rules or other misconduct while using personal devices.
- Maintain confidentiality and ethical standards with respect to information sharing and network security.

Students
- Students must respect and protect:
    - the privacy of others
    - the integrity, availability, and security of all electronic resources
    - the intellectual property of others
    - and practice the principles of community
- Students must comply with the requirements and responsibilities outlined in the MHS BYOD and Cyber Safety User Agreement (also see Guidelines for specific expectations and responsibilities)
- Sign a MHS BYOD User Agreement

Parents and Caregivers
- Ensure that BYOD and student behaviour comply with MHS guidelines
- Co-sign a MHS BYOD and Cyber Safety User Agreement

Marryatville High School BYOD Guidelines

Student Expectations
Users must respect and protect the privacy of others by:
- Using only their own assigned accounts.
- Only viewing, using or copying passwords, and accessing data or networks to which they are personally authorised.
- Refraining from distributing private information about others or themselves.
- Taking full financial responsibility for their device and its maintenance.
- Refraining from touching or tampering with a device that belongs to another person without explicit consent.
- Refrain from using personal hotspots or ad -hoc networks

Users must respect and protect the integrity, availability, and security of all electronic resources by:
- Observing all school internet filters and posted network security practices.
- Reporting security risks or violations to a teacher or network administrator.
- Not destroying or damaging data, networks, or other resources that do not belong to them.
- Conserving, protecting, and sharing these resources with other users
- Notifying a staff member or administrator of computer or network malfunctions immediately.

Users must respect and protect the intellectual property of others by:
- Following copyright laws (not making illegal copies of music, games, or movies).
- Citing sources when using others' work (not plagiarising).

Users must respect and practice the principles of community by:
- Communicating only in ways that are kind and respectful.
- Reporting threatening or discomforting materials to a teacher, leader or administrator.
- Not intentionally accessing, transmitting, copying, or creating material that violates the school's code of conduct (such as messages/content that are pornographic, threatening, rude, discriminatory, or meant to harass).
- Not intentionally accessing, transmitting, copying, or creating material that is illegal (such as obscenity, stolen materials, or illegal copies of copyrighted works).
- Not using the resources to further other acts that are criminal or violate the school's code of conduct.
- Avoiding spam, chain letters, or other mass unsolicited mailings.
- Refraining from buying, selling, advertising, or otherwise conducting business, unless approved as a school project
- Ensuring their device is charged at home (charging is not permitted at school)

Supervision & Monitoring
- The use of digital devices at school is not private.
- School and network administrators monitor the use of information technology resources to help ensure that users are compliant with User Agreements.
- Administrators reserve the right to examine, use and disclose any data found on a student's device or the school's information networks. They may also use this information in disciplinary actions, and will furnish evidence of crime to law enforcement.
- Marryatville High School reserves the right to determine which uses constitute acceptable use and to limit access as deemed appropriate.
- MHS reserves the right to take immediate action if students are using their BYOD for activities:
  - that create security and/or safety issues for the MHS network, Users, schools, network or computer resources;
  - that expend MHS resources on content that lacks legitimate educational content/purpose
  - other inappropriate activities.

Software Installation

- Students may install applications and files onto laptops provided that the installed applications and files:
    - Are appropriately licensed (i.e. they do not breach copyright and intellectual property laws – this includes video and music downloads).
    - Are ethically and morally acceptable (including appropriateness, age appropriate ratings and privacy issues).
    - Do not affect the efficient functioning of the laptops for educational purposes (i.e. they do not interfere with the speed and storage capacity of the laptop or the problems that might arise from increased battery use).
    - Do not affect the school wireless network.
    - Do not interfere with the classroom learning program (i.e. they may only be used in class under specific teacher direction).

Virus Protection

- All students must ensure that they have appropriate virus protection installed on their device. If a student machine attempts to connect to the school network and is found to have a virus the student will be notified immediately and access will be denied until the device has been cleared of any virus. Devices will be scanned on a regular basis.
- Viruses can enter laptops through removable media such as CDs, DVDs, MP3 Players, mobile phones, Bluetooth devices and USB memory sticks, emails, the Internet (including web browsing, FTP programs and chat rooms) To avoid viruses students should:
    - not open any files 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 junk email, commonly referred to as Spam
    - run your virus scan regularly.

Networks & Network Security

- The creation of an Ad-hoc Networks or standalone wireless network between two or more laptops is not permitted.
- Students must not plug any device into the school wired network.
- Hacking is a criminal offence under the Cyber Crime Act (2001)
- Any type of software or hardware device designed to capture or view network data/packets is not permitted.

Charging

- Students must bring the laptop to school each day fully charged. Students will not be permitted to recharge laptops at school.

Damage

- The school takes no responsibility for software, hardware or data loss damage/issues that result from use at school and connecting to the school network
- If a BYOD is damaged students will not be issued with a replacement by the school and must endeavour to repair/replace as soon as possible.

Cancellation

- Students who breach any of the above conditions or agreements (BYOD and Cyber Safety) may have their access cancelled.

Connecting to the BYOD Network

- Students who wish to connect their device to the school wireless network need to complete & return the MHS BYOD & Cyber Safety Agreement forms to Student Services

- BYOD must be presented to the ICT Help Desk (Student Services) for inspection.
- Upon approval (device specifications and agreements) students will be provided with a set of instructions to enable "self on boarding" to the Marryatville High School wireless network.

Required Device Specifications

Aspect	Minimum Specification
Device Type	• Laptop device only (PC or Mac) • Only one device per student
Screen Size	• 11-14 inches
Operating System	• Windows 10 or Apple Mac OSX
Wi-Fi Adaptor	• 802.11 AC capable
Battery Life	• Minimum 7-8 hours
Software	• Students must supply their own software
Other Essential Requirements	• Latest version antivirus

Addition Recommended Device Specifications

Aspect	Minimum Specification
Warranty	• Extended warranty (3years) with Accidental Damage
Storage Capacity	• 128GB of higher SSD Hard Drive
Weight	• We recommend that the weight of the device not exceed 2 kg.
Required Accessories	• Protective case/cover

Access & Technical Support

Access or Support	School Specified Device (Year 8 – 12)	BYOD (Year 11 & 12 only)
Wireless Internet Access	☑	☑
Printing	☑	☑
Access To Daymap	☑	☑
Access to school Network ie.Com Data / Net Apps	☑	☒
Hot Swap if device malfunctions under warranty	☑	☒
Replacement device available for borrowing if damaged and logged for repair	☑	☒
Technical Support (wireless connection only)	☑	☑
Full Technical Support	☑	☒
Arrangement of repairs under warranty	☑	☒
Access to Online Text books	☑	☑

CYBER SAFETY AGREEMENT

The measures to ensure the cyber-safety of Marryatville High School are based on our core values. To assist us to enhance learning through the safe use of information and communication technologies (ICTs), we are now asking you to read this document and sign the attached Use Agreement Form.
Rigorous cyber-safety practices are in place, which include Cyber-Safety Use Agreements for staff and students, who have been involved in the development of the agreement. Child protection education, such as the Keeping Safe child protection curriculum, includes information about remaining safe when using new technologies and is provided to all students.

The computer network, Internet access facilities, computers and other ICT equipment/devices bring great benefits to the teaching and learning programs and to the effective operation of the school. The ICT equipment is for educational purposes appropriate to this environment, whether it is owned or leased either partially or wholly by the school, and used on or off the site.

The overall goal of Marryatville High School is to create and maintain a cyber-safety culture that is in keeping with our values and with legislative and professional obligations. The Use Agreement includes information about your obligations, responsibilities, and the nature of possible consequences associated with cyber-safety breaches that undermine the safety of the school environment.

All students will be issued with a Use Agreement and once signed consent has been returned to school, students will be able to use the school ICT equipment.

Material sent and received using the network may be monitored, and filtering and/or monitoring software may be used to restrict access to certain sites and data, including e-mail. Where a student is suspected of an electronic crime, this will be reported to the South Australia Police. Where a personal electronic device such as a mobile phone is used to capture images of a crime, such as an assault, the device will be confiscated and handed to the police.

While every reasonable effort is made by schools and DECD administrators to prevent student's exposure to inappropriate content when using the department's online services, it is not possible to completely eliminate the risk of such exposure. In particular, DECD cannot filter Internet content accessed by your child from home, from other locations away from school or on mobile devices owned by your child. DECD recommends the use of appropriate Internet filtering software.

CYBER SAFETY AGREEMENT

The use of the Network and access to the Internet from the school is for school authorised purposes only. Students will receive individual logins and passwords for the network and the Internet. A copy of the conditions is set out below:
Your use of the system means that you accept the following conditions of use:

System Conditions
- You will use the curriculum network for school authorised purposes only.
- You will only store appropriate or approved data on the school network.
- You will log on to the system and Internet with your login only.
- You will keep your account passwords secure and not share them with anyone.
- Your login and password is your responsibility, you are liable for any and all activities originating from your account.
- You will store only authorized programs on the school system (NO games, MP3s, movie files, shockwave files or non-approved software).
- You will leave hardware, software, data files and system configurations in the states you find them.
- Accessing chat rooms, forums or instant messaging is prohibited.

- You will not attempt to access data that you do not have permission to access.
- You will not bring to school material that is illegal, inappropriate or offensive to the school ethic or community at large.
- You will not use USB's that are visibly damaged in the school computers.
- You will need to pay for additional printing use at the book room once your initial allocation has been exceeded.

Internet Access Conditions

- You will need to pay for additional Internet use after your allocation has been exceeded.
- You will use the Internet to access only curriculum related materials as specified by the teaching staff.
- You will use information from the Internet appropriately and will not plagiarise this material.
- You will refrain from using offensive or inappropriate language on the Internet or Email.
- You will not access material from the Internet that is offensive, inappropriate or connected with illegal activities.
- You will not send unsolicited, inappropriate, or 'chain letter' Email.
- Internet and Email is not to be used to harass, bully or offend other users.
- You will refrain from downloading software from the Internet.
- You will only use Office365 Pro Plus (OneDrive), or other Cloud based storage spaces (Dropbox, Google Drive, etc) for your school work, and will not use it to store sensitive or personal information.

All student activities on the school network and the Internet are constantly monitored using a comprehensive monitoring system. This helps to maintain a safe computing environment, and to detect breaches of the above conditions.

You are granted full access to our system subject to the above conditions. If these privileges are abused then your privileges may be suspended to some or all of the facilities available at the school. Serious breaches may result in suspension from school and / or payment to restore the system to its original condition.

CYBER-SAFETY USE AGREEMENT

I have read and understood this Cyber-safety Use Agreement and I am aware of the school's initiatives to maintain a cyber-safe learning environment. I understand there will be appropriate consequences in the event of irresponsible behaviour

School: **Marryatville High School**   **Date:** _____

Signed: _____ (student)

Signed: _____ (parent / caregiver)

Date: _____

Please note: This agreement will remain in force as long as your child is enrolled at this school.
If it becomes necessary to add/amend any information or rule, you will be advised in writing.

Return completed agreement form to Student Services

AKNOWLEDGEMENT & AGREEMENT

Name of student: Student ID:

☐ ☐ ☐ ☐ ☐ ☐

We have read and understood the **BYOD Guidelines** with respect to :

☐ **Student Expectations**

☐ **Student Supervision and Monitoring**

☐ **Software Installation**

☐ **Virus Protection**

☐ **Network Security**

☐ **Charging**

☐ **Damage**

for senior students (Year 11 & 12) at Marryatville High School

☐ We declare that our device is compliant with **Device Specifications**

☐ We have read and accept the **level of access and technical support** available for BYOD.

☐ We have read, understood and signed the Marryatville High School **Student Cyber Safety Agreement**

☐ We understand that **BYOD privileges will be cancelled** and there will be appropriate consequences in the event of irresponsible behaviour

School: **Marryatville High School**   Date: _____

Signed: _____ (student)

Signed: _____ (parent / caregiver)

Date: _____

Return completed agreement form to Student Services

Please remove this page from the booklet
Complete & sign all sections
Return at your BYOD appointment