BYOD

(Bring Your Own Device)

Student Agreement

CONTENTS

Further Information: Email IT Support, – itsupport@mabelparkshs.eq.edu.au

OVERVIEW

Student's today face an ever-changing, technologically advanced, global working environment. Therefore, being equipped to use and engage with technology are essential skills to be successful both today and in the future. BYOD roll-out across the school;

Rollout Plan

- 2024 - All Year 7, 10, 11 enrolled in ALL subjects and Year 12 General Subject students
- 2025 - All year 7, 8, 10, 11 and 12 students enrolled in ALL subjects
- 2026 - All students

Please tick one of the following options

☐ OPTION 1: BYOD (Bring Your Own Device)

It is a term used to describe a digital device ownership model where students use their personally owned mobile devices to access the Department's information and communication (ICT) network. The majority of our students take up this free option.

Access to the Department's ICT network is provided only if the device meets the Department's security requirements which, at a minimum, requires that anti-virus software is running and is kept updated on the device.

☐ OPTION 2: School Owned Laptop Hire

We have a limited but adequate number of school owned laptops that we hire on an annual basis to students, with priority given to senior school students. This device is to be returned to the school once the student is no longer a student at Mabel Park State High School or upon school request.

Fee Options

☐ **Upfront** - $100 security deposit and $200 yearly hire fee paid in full ($300 total) before pick up of the device

☐ **Payment Plan** - $100 security deposit paid in full prior to pick up of the device and $200 hire fee paid via payment plan over the school calendar year ($300 total).

Should a school owned laptop be accidentally damaged, misplaced or stolen. The refundable $100 security deposit will be forfeit and additional charges may apply.

BRING YOUR OWN DEVICE (BYOD)

Device Selection

Before acquiring a device to use at school the parent/carer 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 enable class activities, meet student needs, meet network requirements and promote safe and secure network access.

Minimum Hardware Requirements for Device Selection

The device selected by parents **must** meet certain technical requirements. In order to support parents and take the stress out of purchasing, the school website has a device guide & ordering page whereby parents can purchase a device in full confidence that school specifications are met.

A distinct advantage of buying from any of the 2 vendors on our BYOD Portal is that all laptops have 3 years on campus warranty and 3 years accidental damage protection insurance (ADP) can be included.

If purchasing from a store, it is imperative to note the following **minimum specifications** before purchase to avoid wasted expenditure and disappointment:

Operating System Options:

- Windows 10 or later
- MacOS 10.15 or later
- **NOT SUPPORTED:**
  Windows 10 S, Android, Linux/Unix/BSD/*nix, Chrome OS, iOS, iPad OS

Processor: Intel Pentium Quad Core/Intel Dual-Core i3/AMD Ryzen 3 Quad core

Memory: Minimum 8GB RAM

Screen Size: Minimum 11 inch

Hard Drive: Minimum 128GB SSD

Keyboard:

- Must have a tactile (physical) keyboard
- Touch screen keyboard alone is **NOT SUFFICIENT**

Wireless Adaptor:

- Must support 802.11n 5Ghz wireless networks
- ***USB Ports:*** Minimum of 2

Other:

- Hard and/or well-padded protective case
- Consider weight/size factor for student well-being and fitting into school bag.
- The student's account on their laptop must be an administrator.

Support Provided by School

- Mabel Park State High School BYOD agreement will support printing, filtered Internet access, and file access and storage while at school as well as technical support for diagnosis of hardware/software issues on privately owned devices. School IT Support is only able to assist with physical repairs on devices purchased through the BYOD vendor portals on the school website.

Responsibility for Care of Device

- 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 for loss and also for accidental damage if the laptop is purchased from a store retailer rather than from the BYOD Portal.

Software

Main Programs

When a student signs up for BYOD connectivity, the school will provide information and support with respect to the following software packages where agreements have been entered into between Education Queensland and the vendors for the purpose of providing student software for personally owned devices:

- *Microsoft Office* – every student in Education Queensland schools is entitled to download and install Microsoft Office onto a maximum of 5 personal devices for free. DO NOT purchase it.
- *Adobe Creative Cloud* – our students can obtain a free licence for a range of programs in this suite, if required in their school subjects only. This is organised by liaison with classroom teachers at the beginning of the year and again at mid-year.

Suggestions of additional software you may wish to install

- Antivirus software: Although Windows devices have *Windows Defender* as default virus protection, you may wish to install a free antivirus program such as Avast or AVG; or purchase Kaspersky or Bitdefender. Be sure to install only 1 of these – having more than one will cause conflicts.
  N.B. If you install one of these, *Windows Defender* will automatically “step down”.
- We also recommend installing the following free software: Java, Google Chrome, Adobe Reader & VLC Player

GENERAL INFORMATION

Responsibilities of Stakeholders Involved in the Agreement

The School

- Laptop program induction — including information on connection, appropriate digital citizenship and cybersafety
- Network connection at school
- School network and cloud storage
- School email address
- Internet filtering (when connected via the school's computer network)
- Technical support for all students (BYOD limitation as laptop is not school owned)
- Free software - Microsoft Office (all students) and Adobe products (if required in subject)
- Approved online memberships – e.g. Education Perfect, etc.
- Printing facilities and limited print credit ($10 annually)

Student

- Participation in laptop program induction
- Acknowledgement that core purpose of device at school is for educational purposes
- Care of device
- Appropriate digital citizenship and online safety
- Security and password protection – 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
- Maintaining a current back-up of data – especially assessment
- Charging of device – it is expected that students will bring their laptop to school every day, fully charged, in preparation for the next day's classes
- Abiding by intellectual property and copyright laws (including software/media piracy)
- Internet filtering (when not connected to the school's network)
- Ensuring device will not be shared with another student for any reason
- No use of mobile phones to hot-spot to deliberately circumvent the cyber protections put in place for students on campus by Education Queensland
- Understanding and signing the BYOD 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 re-image 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 Agreement

Web Filtering

At all times students, while using ICT facilities and devices, will be required to act in line with the requirements of the school's *Student Code of Conduct*. (school website)

To protect students (and staff) from malicious web activity and inappropriate websites, Education Queensland operates a comprehensive web filtering system with their schools. Any device connected to the Internet through the school network will have filtering applied.

The filtering system provides a layer of protection to students and staff against:

- inappropriate web pages
- spyware and malware
- peer-to-peer sessions
- scams and identity theft

Whilst this filtering approach represents global best-practice in Internet protection measures, despite internal departmental controls to manage content on the Internet, illegal, dangerous or offensive information may be accessed or accidentally displayed. 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.

Privately owned devices have access to home and other out of school Internet services which may not include any Internet filtering. Parents/caregivers are encouraged to install a local filtering application (compatible with the school's network) 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.

In relation to this, students and parents need to be aware of the following:

- Students are not permitted to hot-spot their phones for Internet connectivity, as this negates the very benefits that are designed to protect them from being vulnerable whilst online at school. Students caught doing this will face consequences.
- It is totally unacceptable for students to download programs onto their computer that are designed to circumvent the filtering protection provided by Education Queensland on the school campus.
- Using VPN (Virtual Private Network) software **will** conflict with the school wireless connectivity process – i.e. they will not be able to access the Internet or necessary network drives whilst on campus.

Data Security and Back-ups

- Students must understand the importance of backing up data securely. Should a hardware or software fault develop, important assignment work may be lost.
- The student is responsible for the backup of all data. While at school, students are able to save data to the school's network which is safeguarded by a scheduled nightly backup and therefore strongly encouraged as the most reliable form of backup.
- Education Queensland also provides every student with approximately 2TB of secure cloud storage (*OneDrive*) which of course is accessible on and off campus.
- Whilst other forms of back-up such as USB drives, external hard drives are an option, these do not have the security and reliability of *OneDrive* and the school server. They are volatile in the sense that they can be damaged, data corrupted and are easily misplaced.
- Students who are part of the school laptop hire program or have purchased their laptop from the BYOD Vendor Portal should also be aware that in the event that any repairs need to be carried out on the laptop relating to the hard drive, data stored on the laptop could be lost.

Acceptable Computer and Internet 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 relevant policies of Education Queensland.

Communication through internet and online communication services must comply with the *Student Code of Conduct* available on the school website.

There are conditions that students are required to adhere to. 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 or intentionally download unauthorised software, graphics or music
- intentionally damage or disable computers, computer systems or Queensland DET networks
- use the device for unauthorised commercial activities, political lobbying, online gambling or any unlawful purpose.

Note: Students' use of Internet and online communication services may be audited at the request of appropriate authorities for investigative purposes surrounding inappropriate use.

Passwords

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

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, accessible and 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 behaviour policies also support 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*' on school devices to talk, report and learn about a range of cyber safety issues. Cyber safety is also addressed in Futures lessons throughout the year.

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 recipient's computer
- chain letters, hoax emails or phishing emails
- spam (such as unsolicited advertising).

Students must never send, post or publish:

- 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.

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.

Responsible Use of ICT Devices

Our goal is to ensure the safe and responsible use of facilities, services and resources available to students through the provision of clear guidelines.

- ICT devices on campus should be primarily used for engagement in class work and assignments set by teachers, conducting general research for school activities and projects and communicating or collaborating with other students, teachers, parents, caregivers or experts for educational purposes.
- 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.
- 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 behavior policies.
- The school will educate students on cyber bullying, safe Internet and email practices. Students have a responsibility to incorporate these safe practices in their daily behaviour at school.
- 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.

When using ICT devices, students **MUST NOT**:

- use the device in an unlawful manner
- create or participate in circulating 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
- download (or using unauthorised software for), distributing or publishing of offensive messages or pictures
- use obscene, inflammatory, racist, discriminatory/derogatory or bullying language
- download viruses/other programs capable of breaching the Department's network security
- use the ICT device's camera or recording functions inappropriately, violating the privacy of other individuals

- covertly use Bluetooth functionality during lessons or exams
- hotspot their phone to bypass the school's protective filtering designed to ensure cyber safety
- 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.

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. Students must not trespass 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 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 and be subject to prosecution from agencies to enforce such copyrights.

PARENTAL CONFIRMATION

For the commencement of the school year, all parents/carers will be required to complete a short online information/consent form which will be emailed to parents/carers at the end of the year and repeated at intervals as required (newer enrolments/no responses) until the start of the school year. For enrolments after this time, please refer to the printed single page document in your enrolment package entitled ***BYOD Agreement for Parents & Carers***. The purpose of this document is stated below:

Acceptable Use Policy – your child's and your acceptance of computer/Internet usage on the school campus; and

Preferred Option for Your Child – informs us of your decision for your child's laptop option, so that we will be prepared and provide further relevant advice to you, based on your decision.

1. BYOD (bring own laptop) – free connection to network
2. School hire laptop for the year - $200 p.a. + $100 security deposit
   - Upfront
   - Payment Plan

The following is to be read and completed by both the STUDENT and PARENT/CAREGIVER and both pages returned to the school.

Student:

- I have read and understand the BYOD Agreement and I agree to abide by the guidelines outlined in this document.
- I understand that the school will not repair my BYOD device hardware or operating system software, and that technical support is limited to network connection and provision of school-based software.
- I am aware that non-compliance or irresponsible behaviour, as per the intent of the BYOD Agreement and Mabel Park State High School's Student Code of Conduct, will result in consequences relative to the behaviour.
- I understand that the school's information and communication technology (ICT) facilities and devices provide me with access to a range of essential learning tools, including access to the internet. I understand that the internet can connect me to useful information stored on computers around the world.
- While I have access to the school's ICT facilities and devices: I will use it only for educational purposes; I will not undertake or look for anything that is illegal, dangerous or offensive; and I will not reveal my password or allow anyone else to use my school account.
- Specifically, in relation to internet usage, should any offensive pictures or information appear on my screen I will close the window and immediately inform my teacher quietly, or tell my parents/guardians if I am at home.
- If I receive any inappropriate emails at school, I will report this to my teacher. If I receive any at home, I will report this to my parents/guardians. When using email or the internet I will not:
    - reveal names, home addresses or phone numbers – mine or that of any other person
    - use the school's ICT facilities and devices (including the internet) to annoy or offend another person
- I understand that my online behaviours are capable of impacting on the good order and management of the school whether I am using the school's ICT facilities and devices inside or outside of school hours.
- I understand that if the school decides I have breached the rules for using its ICT facilities and devices, appropriate action may be taken as per the school's Student Code of Conduct, which may include loss of access to the network (including the internet).

I have read and understood this Agreement and the Student Code of Conduct. I agree to abide by the above Agreement.

Student Name:	Parent/carer name:
Signature of student:	Signature of parent/carer:
Date:	Date:

Parent or guardian:

- I understand that the school provides my child with access to the school's information and communication technology (ICT) facilities and devices (including the internet) for valuable learning experiences. In regards to internet access, I understand that this will give my child access to information on computers from around the world; that the school cannot control what is on other computers; and that some of that information might be illegal, dangerous or offensive.
- I accept that, while teachers will always exercise their duty of care, protection against exposure to harmful information should depend upon responsible use by students/my child. Additionally, I will ensure that my child understands and adheres to the school's appropriate behaviour requirements and will not engage in inappropriate use of the school's ICT facilities and devices. Furthermore, I will advise the school if any inappropriate material is received by my student/child that may have come from the school or from other students.
- I understand that the school does not accept liability for any loss or damage suffered to personal mobile devices as a result of using the department's facilities and devices. Further, no liability will be accepted by the school in the event of loss, theft or damage to any device unless it can be established that the loss, theft or damage resulted from the school's/department's negligence.
- I believe my child understands this responsibility, and I hereby give
- my permission for them to access and use the school's ICT facilities and devices (including the internet) in accordance with school requirements.
- I understand where inappropriate online behaviours negatively affect the good order and management of the school, the school may commence disciplinary actions in line with this user agreement or the Student Code of Conduct. This may include loss of access and or device and usage of the school's ICT facilities and devices.
- I have read, understood and will abide to this Agreement and the Student Code of Conduct.

Parent/carer name:
Parent/carer signature:
Date:

Trent Cowely
Executive Principal
Mabel Park State High School

NOTE: PLEASE RETURN TO THE SCHOOL FINANCE WINDOW