BYOD HANDBOOK

Ripley Central State School

Passion & Purpose

Contents

WHAT IS BYOD?

Bring Your Own Device (BYOD) is a term used to describe a digital device ownership model where students use their privately-owned devices to access the departmental networks and information management systems in an educational setting.

Devices are used in the classroom to enhance students' learning experiences in accordance with the Department of Education's 21st Century learning guide. The purpose of BYOD is to create and maintain a highly engaging learning environment that equips students with the capacity to think, solve problems, respond to and thrive within a changing society. A blend of traditional and digital learning approaches will be integrated to maximise the learning potential of every child. The use of technology as a tool, extends learning opportunities for all students combined with normal books, pencil, pen and paper to form the basis of the daily class routine.

Consultation with prospective families at our community meeting held in September 2022, saw an overwhelming support for BYOD implementation from Year 2 to Year 6; with iPads as the preferred device for Years 2 to 4 and laptops for Years 5 and 6. To support families with the outlay of costs, a phased implementation approach will be taken by our school – refer to the table below.

	2023	2024	2025
Prep			
Year 1			
Year 2		BYOD iPad	BYOD iPad
Year 3		BYOD iPad	BYOD iPad
Year 4			BYOD iPad
Year 5		BYOD Laptop	BYOD Laptop
Year 6			BYOD Laptop

IN 2024

Students in Year 2 and 3 will need to acquire an iPad to support their learning and students in Year 5 will need a Windows laptop to support their learning.

PURPOSE

The BYOD program is integral to our belief of fostering a progressive, adaptive, and immersive learning environment at our school. This initiative, designed for students in Years 2 to 6, aims to meld cutting-edge technology with conventional educational resources, crafting a vibrant learning ecosystem reflective of real-world scenarios. The program is focused on ensuring that students in Years 5 and 6 are proficiently equipped with the digital skills and acumen essential for high school.

With this program, students in Years 2 to 4 will integrate the use of iPads, while those in Years 5 and 6 will utilise Windows laptops, catering to their unique learning and communicative styles. This strategy encourages personalised education and grants families the liberty to make informed decisions about device selections, adhering to specified guidelines. In this era of rapid technological advancement, our goal is to enrich the educational journey, foster critical thinking, and prepare our students to flourish in an ever-evolving world. By harmonising a blend of digital and traditional pedagogies, we are committed to shaping a generation of learners who are poised and prepared for the future.

DEVICE SELECTION

Before acquiring a device to use at school the parent or caregiver 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 enabling class activities, meeting student needs and promoting safe and secure access to the department's network.

Devices can be purchased from any retail or online store. Alternatively, devices can be purchased in store or online via a number of BYOD portals, this information can be located on our website.

DEVICE SPECIFICATIONS

iPads (Year 2 and 3)

We recommend a minimum of 64gb storage and capable of running the latest version of iOS16.4.1(a), (operating system for iPads). Currently, this includes the 7th gen, 8th gen, iPad Air 2, iPad Pro. *The iPad mini does NOT meet minimum requirements.

Cellular iPads with a SIM installed will not be accepted. All students will have access to filtered Department of Education Wi-Fi at school.

iPad Setup - Parents should refer to the web site for instructions on how to prepare the iPad for school and setting up their child's iPad and the Intune Company Portal app to access the school Wi-Fi network and install learning applications.

Case Recommendations - We strongly recommend a robust case to minimise potential damage as well as a glass screen protector.

Insurance - AppleCare, Warranty and/or Accidental Damage Protection is recommended – please note you may need to articulate the device/s in your Policy to ensure that the device is covered for usage outside of the home.

Laptops (Year 5 students)

Devices that support Windows operating systems will provide students with the most advantage. Some devices such as Chromebooks and Android devices will not connect to the BYOD network and we will not be able to provide technical support to these devices. There are a range of devices that meet the device specification requirements.

<u>MINIMUM SPECIFICATIONS</u>

Non-Technical Subjects and Primary School Students

- Intel Core i3 or AMD Ryzen 3. Dual Core or higher
- Intel HD Graphics 5000
- 8Gb RAM
- 256Gb Hard Drive (note: we recommend a 256Gb or higher Solid-State Drive for increased durability and speed)
- 13" or larger display
- Wireless Network 5Ghz
- Battery sufficient to last 6 hours on Balanced Power Mode
- Windows 64bit Operating System. NOTE: Windows 10 S is not compatible.
- USB Ports
- Virus Protection (Certain antivirus software are not recommended. See below for more information.)

Laptop Devices with Cellular Data will not be accepted in the BYOD program.

INSURANCE

Purchasing insurance is a personal choice – we highly recommend this. When purchasing your device please check your options to purchase accidental damage protection for your device. Ensure that this covers your device for accidental damage on and off the school campus. Fire, Theft and Natural Disasters are usually not covered under these programs, but you can include it in your personal or home insurance. The insurance can be purchased with your computer vendor or any insurance company. All insurance claims must be settled between you and the insurance company.

DEVICE LOSS AND DAMAGE

- Digital devices will be the responsibility of the student (owner).
- The School accepts no responsibility for the security or safety of the device.
- We advise that all devices are covered by an extended warranty to last the student's time at Ripley Central State School.

REQUIRED SOFTWARE

Our school has recommended software applications in order to meet the curriculum needs of particular subjects.

- **Antivirus:** Reputable antivirus software is advised.
  Please note that the following Antivirus' may prevent your device from accessing our network and are therefore not recommended:
  - McAfee Antivirus
  - TrendMicro
  - Avast AntiVirus
- **Office 365 and other Apps to support learning:** All software to support learning will be available to download at no cost for students. This includes Microsoft Office and Minecraft Education. Parents/caregivers will be required to install and support the appropriate use of the software via the app 'Intune Company Portal.' Information on how to download required software is available on our school website. Teachers will also be providing lessons on how to access this software.

CARE OF DEVICE

The student is responsible for taking care of and securing the device and accessories in accordance with school 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. 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.

General precautions:

- Food or drink should never be placed near the device.
- Plugs, cords and cables should be inserted and removed carefully.
- Devices should be carried within a robust protective case where appropriate.
- Carrying devices with the screen open should be avoided.
- Each device and accessories should be clearly labelled with the student's name.
- Turn the device off before placing it in its bag.

BATTERY LIFE & DEVICE CHARGING

The device is expected to come to school fully charged. To minimise accidental loss of property, bringing the device charger to school is not required.

Tips to Increasing Battery Time:

- Reduce the screen brightness to a comfortable level.
- Disable connectivity such as Wi-Fi and Bluetooth when not in use.
- Close all running apps/programs when not in use.

BYOD SECURITY

Students will have their device secured in their classroom during all lunch breaks and will not have access to them during this time.

When the classroom teacher is absent, the device will not be used for the day and will remain locked in a secure cupboard.

ON-BOARDING

On boarding is the process of enrolling your device to Microsoft Intune which lets your laptop or iPad to connect to the school network and access to the available shared network resources. At the beginning of each year and during the first 4 weeks of Term 1, teachers and Technical Support staff will assist students to complete this process at school.

Must do before On-boarding

The checklist below should be followed for each device that is to connect to the BYOD network prior to bringing the device to school.

- ☐ **Check for Windows updates through Control Panel**. Download and install them is available. Onboarding will not be successful until this is complete.
- ☐ Completely shut down the laptop and restart it while connected to your network at home. This is to make sure the laptop has received and applied all updates.
- ☐ Ensure the account the student uses to log onto the laptop is an administrator account.
- ☐ Time and date is correct.
- ☐ An up-to-date anti-virus is installed.

TECH SUPPORT

Our school will offer a range of support to our families including information evenings, online resources, newsletter articles and website updates. Additionally, opportunities will be provided on topics that will support safe use of devices for both students and parents. Some events may include student led sessions to showcase student learning and upskill parents in the many activities students engage in with their devices.

Teachers will be able to provide basic technical assistance to students such as connecting to the internet, basic troubleshooting, and advice on where more extensive work or repairs may be needed. Teachers will continue to be trained on how to best utilise technology to enhance the learning experience and learning outcomes of their students.

It may become necessary for students to restore their device using recovery software supplied in the box or by following another reset procedure. In these cases, students will need to take the device home and follow the recovery instructions provided by the vendor. Before restoring the computer make sure all of the data has been backed up to an external device.

All warranty issues are to be addressed through individual suppliers. All legal liability of the device in terms of loss, damage or theft is also the responsibility of the owner and not the school.

For school-based technical support with device set up or questions, please email BYOD@ripleycentralss.eq.edu.au

ACCEPTABLE PERSONAL MOBILE DEVICE 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 policy contained within the Acceptable Use of the Department's Information, Communication and Technology (ICT) Network and Systems. The acceptable-use conditions apply to the use of the device and internet both on and off the school grounds.

The fundamental purpose of personal mobile devices within our school is to facilitate a dynamic and interactive learning environment, leveraging technology to enhance educational outcomes, promote creativity, and foster communication. These devices are intended to be used as tools to access educational resources, perform research, complete assignments, and collaborate with peers and educators.

Any utilisation of these devices that deviates from this core educational objective may be considered a breach of effective use. This includes, but is not limited to, any activities that undermine the security and integrity of hardware and software systems, unauthorised downloading or modification of content, intentional damage to systems, and using the device for any activities that are commercial, political, unlawful, or inconsistent with the department's Code of School Behaviour and the School's Student Code of Conduct. It is imperative that the use of personal mobile devices aligns with the guidelines and policies outlined by the Queensland Department of Education to maintain a secure, respectful, and conducive learning environment for all.

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.

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.

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, or suspended.

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 and accessible. This content 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 Student Code of Conduct also supports students by providing school related expectations, guidelines and possible consequences.

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. At all times students, while using ICT facilities and devices, will be required to act in line with the requirements of the Student Code of Conduct) and any specific rules of the school.

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

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.

The personally-owned devices have access to home and other out of school internet services and those services may not include any internet filtering. Parents and caregivers are encouraged to install a local filtering application 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. Parents, caregivers and students are also encouraged to visit the website of the Australian eSafety Commissioner for resources and practical advice to help young people safely enjoy the online world.

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, including not trespassing 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.

EQUITY BANK

If parents opt not to provide a personal device due to financial hardship, students may have access to a shared school owned device for use in the classroom from our Equity Bank. These devices are school owned, and as such, will not be permitted to go home with the student. To enquire about our Equity devices, please email BYOD@ripleycentralss.eq.edu.au.