Warrigal Road State School

Bring Your Own Device (BYOD) Program

Information and Procedures Handbook

The *Bring Your Own Device (BYOD)* handbook has been developed as a guide for parents and students bringing their own device at Warrigal Road State School. Each family should thoroughly read and understand the content and procedures. By joining the BYOD program, you are agreeing to provide a suitable device for your child's learning.

The BYOD program at Warrigal Road State School enables students to bring their personal devices to school. The emphasis is upon students having the opportunity to access digital technology to enable differentiated personal learning. It is important to remember that digital technology is a tool for learning. Learning occurs when your child engages with content and masters skills in a meaningful and effective manner.

Bring Your Own Device Implementation Plan:

Year	Prep	Year 1	Year 2	Year 3	Year 4-6
2024	School shared devices	Bring your own iPad	School shared devices	School shared devices	Bring your own laptop
2025	School shared devices	Bring your own iPad	Bring your own iPad	School shared devices	Bring your own laptop
2026	School shared devices	Bring your own iPad	Bring your own iPad	Bring your own iPad	Bring your own laptop

PLEASE NOTE: *For students who have financial hardship, there are options available. Please discuss options with your year level Deputy Principal*

CURRICULUM

The Australian Curriculum supports students to meet the demands of the 21st century by providing them with opportunities to become successful learners, confident and creative individuals, and active and informed community members. The general capabilities, together with the learning areas and the cross-curriculum priorities, form part of the Australian Curriculum's three-dimensional curriculum design. Through embedding the general capabilities in Prep to Year 10, schools can equip their students with the knowledge, skills, behaviours and dispositions they need now and for the future. Digital Literacy is one of the general capabilities in the Australian Curriculum (V9).

Digital literacy encompasses the knowledge and skills students need to create, manage, communicate and investigate data, information and ideas, and solve problems. It assists students to work collaboratively at school and in their lives beyond school.

Digital literacy involves students critically identifying and appropriately selecting and using digital devices or systems, and learning to make the most of the technologies available to them. Students adapt to new ways of doing things as technologies evolve, and protect the safety of themselves and others in digital environments.

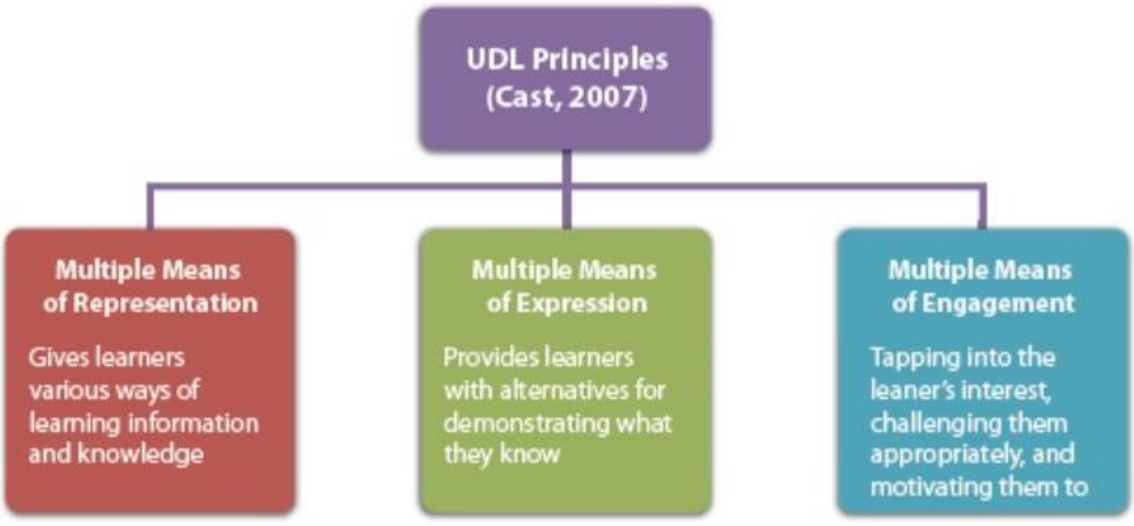
The Digital Literacy learning continuum is organised into 4 elements, as shown in Figure 1:

- Practising digital safety and wellbeing
- Investigating
- Creating and exchanging
- Managing and operating

Figure 1: Digital Literacy elements

UNIVERSAL DESIGN FOR LEARNING

Universal design for learning (UDL) is a teaching approach that works to accommodate the needs and abilities of all learners and eliminates unnecessary hurdles in the learning process. This means developing a flexible learning environment in which information is presented in multiple ways, students engage in learning in a variety of ways, and students are provided options when demonstrating their learning.



ASSISTIVE TECHNOLOGY

Assistive technology has widespread acceptance as a support strategy within international, national and state initiatives. In the education context, research recognises the potential of assistive technology to support access to learning, engagement and achievement for a range of students with diverse learning needs.

Assistive technology in education is any hardware, software or system of technical components and processes that enhances the capacity for all students to engage more effectively with the curriculum and their learning environment. This can range from "high tech" technology, such as electronic devices or power wheelchairs, to "low tech" devices such as a pencil grip, supportive seat or a simple switch.

Assistive technology can support teachers to provide teaching and learning that is accessible to all students. Assistive technology supports students with diverse learning needs within an inclusive learning environment by:

- delivering information to students in a way that is more appropriate to their needs
- changing the way a student can interact with the curriculum and their environment
- providing a more appropriate and accessible way for students to demonstrate their knowledge and understanding of the curriculum.

RESPONSIBILITIES

STUDENTS	PARENTS	SCHOOL
Bring device fully charged each day	Provide a suitable device	Provide suitable school Wi-Fi connection and filtering system
Ensure device is transported in an approved protective case	Maintain the device	Provide a Universal Design for Learning approach, and opportunities for devices to be used as a tool for learning when appropriate
Show respect for others' devices, work and privacy	Install software	Explicitly teach safe device and internet practices (cyber safety)
Be a Responsible User	Provide appropriate insurance and warranty	Provide access to peripheral devices (eg printers)

CYBERSAFETY

All students in the BYOD Program will participate in Cyber Safety and Cyber Bullying education sessions.

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' to talk, report and learn about a range of cybersafety issues.

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 recipients' computer
- chain letters or hoax 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.

Parents, caregivers and students are encouraged to read the department's Cybersafety and Cyberbullying guide for parents and caregivers.

APPROPRIATE DEVICE USAGE

It is an expectation of Warrigal Road State School that all students abide by the Student Usage of the Internet, Intranet and Extranet Policy.

What is acceptable/appropriate use/behaviour by a student?
Students are to use devices and network infrastructure for assigned class work set by the teacher, solely for educational purposes.

What is unacceptable/inappropriate use/behaviour by a student?
It is unacceptable for students to download, distribute or publish offensive messages or pictures; use obscene or abusive language to harass, insult or attack others; deliberately waste printing or internet resources; damage computers, printers or the network equipment; violate copyright laws which includes plagiarism; use unsupervised internet chat (e.g Discord and Skype); and use online email services (e.g. Outlook) to send chain letters or Spam email (junk mail), particularly during class. Students cannot use another student or staff member's username or password to access the school's network, including access to another person's files, home drive or email. Additionally, students should not divulge personal information (e.g.name, parent's name, address), via the internet or email, to unknown entities or for reasons other than to fulfil the educational requirements of the school.

BEFORE AND AFTER SCHOOL USAGE

Once the students have arrived at school, they are not allowed to use their devices until they are in class and have teacher permission.

Students using their devices at Outside School Hours Care should follow the directions of supervisors and follow all school device procedures.

COMPUTER GAMES

Students are NOT permitted to download games onto devices or play computer games at school, as the devices are to be used solely for educational purposes. Students are not permitted to keep games on USBs or other storage devices.

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

Communication through internet and online communication services must also comply with the department's Code of School Behaviour and the Student Code of Conduct available on the school website.

While on the school network, 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 and intentionally download unauthorised software, graphics or music
- intentionally damage or disable computers, computer systems, school or government 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

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 be prompted to change periodically. The password can also be prompted to change by IT personnel at their discretion.

Personal accounts are not to 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 device.

Students should also set a password for access to their BYOD device and keep it private.

Parents/caregivers may also choose to maintain a password on a personally-owned device for access to the device in the event their student forgets their password or if access is required for technical support. Some devices may support the use of parental controls with such use being the responsibility of the parent/caregiver.

VIRUS PROTECTION

Files exchanged between computers outside the school network should be checked for viruses or other malicious software before being transferred and opened. Home computers should have effective virus and spyware protection filters before exchanging files with USB or other file storage used on the school network. Windows 10/11 Defender is a sufficient antivirus and comes free with the operating system (Please ensure Windows Defender updates are enabled).

Please do **NOT** install Total Defense, Total AV, Comodo Cloud Antivirus, Trend Micro Maximum Security or McAfee. Many family versions of antiviruses are also problematic in the school network.

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 Responsible Behaviour Plan also supports students by providing school related expectations, guidelines and 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. 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 Australian Communications and Media Authority's CyberSmart website 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.

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.

MONITORING STUDENT MACHINES FOR SOFTWARE INFRINGEMENTS, INAPPROPRIATE AND OFFENSIVE MATERIALS (Device AUDIT)

Students may be selected on a random basis to provide their device and or USB for inspection for compliance with school requirements. They 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.

DEVICE CARE

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.

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.

REPAIRS AND MAINTENANCE

All maintenance for the devices, operating system, software and/or apps purchased by the family are the responsibility of the family. Families should ensure quick maintenance turnaround for student devices to minimise disruption to learning.

INSURANCE AND WARRANTY

Families are strongly encouraged to have insurance and warranty on personal devices. All reasonable care will be taken; however, it is the responsibility of the family to repair or replace damaged or lost devices.

SCHOOL TECHNICAL SUPPORT

If you experience difficulties, we advise students to report the issue to their class teacher. If the problem cannot be easily resolved, it will be discussed with the school technician and a recommendation will be communicated with the family. (eg. warranty claim, insurance claim etc.) School technicians can assist with issues such as connecting the device to Wi-Fi, however, cannot support repairs and maintenance on individual devices.

BYOD EXPECTATIONS

When should a device be brought to class?

Unless specifically advised otherwise by their teacher, students should bring their device every day. Many lessons will require opportunities for students to use a device to complete tasks. It is imperative that the device be available for use at the teacher's discretion.

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 their protective case where appropriate.
- Ensure the battery is fully charged each day.
- Turn the device off before placing it in its bag.

Wi-fi

Devices that meet the outlined specifications will recognise the school's Wi-Fi network and will be able to connect. Standard EQ internet security filters will screen usage and access whilst at school. **3/4G ability should be disabled in all devices** as this function when activated allows students to bypass the EQ internet security filters. The school will take no responsibility for the content accessed by students using 3/4G facility on their personally owned devices.

IPADS

Identification

iPads, protective cases and chargers should be clearly labelled with students' names. It is encouraged that families create iPad wallpaper (background) with the student's name. Families are responsible for creating a 4-digit pin code for their child's device. Ensure your child knows this pin code.

Charging and transport

iPads are to be charged at home each day and be brought to school fully charged. As well as it being a Workplace Health and Safety issue, there is no provision in classrooms for students to charge devices. An uncharged device will impact on learning that day. Students are to transport iPads to and from school in school bags. All iPads require a screen protector and sturdy, rubberised protective case. A protective carry bag is strongly recommended. iPads will remain in classrooms for the duration of the school day.

LAPTOPS

Identification

Laptops, mouse, USB, chargers and carry cases should be clearly labelled with students' names. Students will log in using their MIS ID (school log in details). Students are responsible for remembering their username and passwords. Staff are able to reset student passwords on request.

Charging and transport

Laptops are to be charged at home each day and be brought to school fully charged. Check Device Specifications for battery life reference or consult your technical support. As well as it being a Workplace Health and Safety issue, there is no provision in classrooms for students to charge devices. An uncharged device will impact on learning that day. Students are to transport laptops to and from school in protective carry bags. Laptops will remain in classrooms for the duration of the school day.

Protecting the laptop screen

- Avoid poking at the screen — even a touch screen only requires a light touch.
- Don't place pressure on the lid of the device when it is closed.
- Avoid placing anything on the keyboard before closing the lid.
- Avoid placing anything in the carry case that could press against the cover.
- Only clean the screen with a clean, soft, dry cloth or an anti-static cloth.
- Don't clean the screen with a household cleaning product.
- Avoid carrying laptops with the screen open

Data security and back-up of data

Students must ensure they have a process of backing up data securely. Otherwise, should a hardware or software fault occur, student work may be lost.

The student is responsible for the backup of all data. While at school, students may be able to save data to the school's network, which is safeguarded by a scheduled backup solution. All files must be scanned using appropriate anti-virus software before being downloaded to the department's ICT network.

Students are also able to save data locally to their device for use away from the school network. The backup of this data is the responsibility of the student and should be backed-up on an external device, such as an external hard drive or USB drive.

Students should also be aware that, in the event that any repairs need to be carried out the service agents may not guarantee the security or retention of the data. For example, the contents of the device may be deleted and the storage media reformatted.

Digital Services Provided By The School

The full Microsoft Office Suite is provided by Education Queensland and is available to download for students and is a mandatory requirement for their BYO Device. Obtaining this can be done by a number of various methods. However, it is best attained by following the Intune onboarding guide below.

INTUNE & ENROLLING A BYO DEVICE

The videos below will give a detailed guide on installing the Company Portal which will link your student's device to Education Queensland Intune management system. Failure to enrol the device will not allow the BYO Device to connect to the schools Wi-Fi.

- BYOxLink - How to guide - iOS - Enrol your BYO device into Intune

https://mediasite.eq.edu.au/mediasite/Play/bbe46710d2c24274a0a99c ba446a92031d

- BYOxLink - How to guide - Windows - Enrol your BYO device into Intune

https://mediasite.eq.edu.au/mediasite/Play/715e41cecde3404488298ec ca633f6ad1d

For further information regarding Intune enrolment please refer to documents supplied regarding How to Guide.

BYOD Year 1 iPad Requirements 2024

Only iPad Generation 7 or later (Devices must support Apple Software updates to ensure compliance with specific apps required)
✓ Wi-Fi capability ✓ Screen protector ✓ Rubberised protective case
× No iPad mini/ iPad Air/ iPad Pro × No Android tablets × No Cellular data

Headphones

The headphones purchased through the Student Resource Scheme in Prep will go with your child to Year 1. You may choose to purchase new headphones, depending on their condition. The following table shows headphone jack requirements for iPads:

Generation 7-9	**Generation 10+**
3.5mm requirement for headphones	USB-C to 3.5mm headphone jack adapter (No built-in jack)
	

BYOD Year 4 Laptop Requirements 2024

	Minimum	Optimal	Above	DO NOT USE
Processor	Intel i3 4th Generation and/or AMD A8-7050 or higher	Intel i5 5th Generation and/or AMD A9-9400	Intel i5 5th Generation and/or AMD A9-9400 or higher	Macbooks
Ram	8GB	8GB	16GB	Ipads
Storage	125GB	256GB	500GB+	Chromebooks
Size	10″	12″-14″	15″	Budget Laptops
Battery	5Hrs+	5Hrs+	5Hrs+	

Must Have:

- ✓ Screen protector
- ✓ Carry Case

Other Considerations:

- ✓ Dual channel wireless
- ✓ Minimum of 2 USB ports (be aware of USB-C and appropriate headphones/accessories to support USB-C)
- ✓ Headphones from Year 3 SRS will go with your child to Year 4. You may choose to purchase new headphones for your child. Suitable examples of headphones:
  - Keji PC Headset
  - Hp Boom Mic Headset 150
  - Verbatim USB Headset with Boom Mic Grey
- ✓ Appropriate carry bag
- ✓ If using a windows tablet consider a protective case
- ✓ Insurance is strongly recommended
- ✓ Family is responsible for sourcing repairs or replacement of damaged or lost devices

Examples** of suitable devices	
Minimum	HP 50R82PA 15.6” HD laptop (256GB) [AMD3050U] Lenovo IdeaPad Slim 3 15.6” (256GB) [Ryzen 3]
Optimal	Dell Inspiron 3505 15.6" Full HD Laptop (512GB) [Ryzen 5] HP Pavilion 14" Full HD 2-in-1 Laptop (256GB) [Intel i5]
Above	HP Victus 16-d0224TX 16.1" FHD 144Hz Laptop (Intel i5) [RTX 3050 Ti]

***Please note these are examples only. We cannot specify the product or where to purchase the device. This is the parent's responsibility.) We are unable to recommend one particular device over another due to our adherence to the 'Public Sector Ethics Act 1994' where we have a 'duty to provide advice which is objective, independent, apolitical and impartial'. Therefore, any device listed below is not our RECOMMENDATION just a guide on which devices are suitable for the QED environment and as such some EXAMPLES from numerous manufacturers are listed below. Furthermore, we cannot recommend one such brand over another only devices which are suitable for QED use.*

Checklist

PREPARING YOUR STUDENT TO BRING THEIR DEVICE TO SCHOOL

- ☐ Set up device following Intune enrolment guide
- ☐ Ensure that your child understands that they are **NOT to share** their device with other students.
- ☐ Ensure that your child understands that they are **NOT to capture photos, video or audio** unless advised to do so by their class teacher.
- ☐ Purchase a **protective case/carry bag** for your child's device, which protects the device from moisture and bumps.
- ☐ Discuss, sign and submit the WRSS ICT Responsible Use Policy Agreement Form

Bring Your Own Device (BYOD) Responsible Use Policy

The main purpose of the Warrigal Road State School 'Responsible Use Policy' is to encourage the mature and responsible use of the facilities available to the students through the provision of clear usage guidelines. Students authorised to use the school's wi-fi network also have Internet and Electronic Mail access.
The use of devices and systems has been designed to help students keep up with the demands of the 21st century. Helping students become responsible digital citizens will enhance not only what we do in the classroom, but also give students skills and experiences that will prepare them for their future studies and career.

RESPONSIBILITIES OF STAKEHOLDERS INVOLVED IN THE BRING YOUR OWN DEVICE (BYOD) PROGRAM:

School

- BYOD Program induction — including information on (but not responsible for) connection, care of device at school, workplace health and safety, appropriate digital citizenship and cyber safety
- network connection at school
- internet filtering (when connected via the school's computer network)
- some technical support (troubleshooting, connectivity)
- some school-supplied software eg apps, programs
- printing facilities

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 (for more details, see ACMA CyberSmart)
- 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 (e.g. a student should not share their username and password with fellow students)
- maintaining a current back-up of data
- charging of device
- abiding by intellectual property and copyright laws (including software/media piracy)
- internet filtering (when not connected to the school's network)
- ensuring personal login account will not be shared with another student, and device will not be shared with another student for any reason
- understanding and signing the Technology 4 Learning Responsible Use Policy Agreement.

Parents and caregivers

- participation in Technology 4 Learning Program induction
- 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 cybersafety with students (for more details, see ACMA CyberSmart)
- some technical support
- 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 Technology 4 Learning Responsible Use Policy Agreement.

THE FOLLOWING ARE EXAMPLES OF RESPONSIBLE USE OF DEVICES BY STUDENTS:

- Use mobile devices for:
  - engagement in class work and assignments set by teachers
  - developing appropriate 21st Century knowledge, skills and behaviours
  - authoring text, artwork, audio and visual material for publication on the Intranet or Internet for educational purposes as supervised and approved by school staff
  - conducting general research for school activities and projects
  - communicating or collaborating with other students, teachers, parents, caregivers or experts as part of assigned school work
  - accessing online references such as dictionaries, encyclopaedias, etc.
  - researching and learning through the school's eLearning environment
  - ensuring the device is fully charged before bringing it to school to enable continuity of learning.

- Be courteous, considerate and respectful of others when using a mobile device.
- Switch off and place out of sight the mobile device during classes, where these devices are not being used in a teacher directed activity to enhance learning.
- Seek teacher's approval where they wish to use a mobile device under special circumstances.

THE FOLLOWING ARE EXAMPLES OF IRRESPONSIBLE USE OF DEVICES BY STUDENTS:

- using the device in an unlawful manner
- creating, participating in or circulating content that attempts to undermine, hack into and/or bypass the hardware and/or software security mechanisms that are in place
- disabling settings for virus protection, spam and/or internet filtering that have been applied as part of the school standard
- downloading (or using unauthorised software for), distributing or publishing of offensive messages or pictures
- using obscene, inflammatory, racist, discriminatory or derogatory language
- using language and/or threats of violence that may amount to bullying and/or harassment, or even stalking
- insulting, harassing or attacking others or using obscene or abusive language
- deliberately wasting printing and Internet resources
- intentionally damaging any devices, accessories, peripherals, printers or network equipment
- committing plagiarism or violate copyright laws
- using unsupervised internet chat
- sending chain letters or spam email (junk mail)
- accessing private 3G/4G networks during lesson time
- knowingly downloading viruses or any other programs capable of breaching the department's network security
- using the mobile device's camera anywhere a normal camera would be considered inappropriate, such as in change rooms or toilets
- invading someone's privacy by recording personal conversations or daily activities and/or the further distribution (e.g. forwarding, texting, uploading, Bluetooth use etc.) of such material
- using the mobile device (including those with Bluetooth functionality) to cheat during exams or assessments
- take into or use mobile devices at exams or during class assessment unless expressly permitted by school staff.

IN ADDITION TO THIS:

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.

- Students using the system must not 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 and without them present.
- Students must not record, photograph or film any students or school personnel without the express permission of the individual/s concerned and the supervising teacher.
- Students must get permission before copying files from another user. Copying files or passwords belonging to another user without their express permission may constitute plagiarism and/or theft.
- Students need to understand 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.
- 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 Warrigal Road State School Responsible Behaviour Plan.
- The school will educate students on cyber bullying, safe internet and email practices and health and safety regarding the physical use of electronic devices. Students have a responsibility to incorporate these safe practices in their daily behaviour at school.

The school's BYOD Program supports personally-owned mobile devices in terms of access to:

- printing
- internet
- file access and storage
- support to connect devices to the school network

However, the BYOD Program does not support personally-owned mobile devices in regard to:

- technical support (repairs)
- charging of devices at school
- security, integrity, insurance and maintenance
- private network accounts

INAPPROPRIATE BEHAVIOUR OUTSIDE OF SCHOOL HOURS

Students may receive disciplinary consequences for bullying or cyberbullying or other inappropriate online behaviour that occurs out of school hours, and affects the good order and management of the school.

All of these policies and protocols apply to USB drives and external hard drives brought into the school.

Misuse of BYOD device or school devices will result in consequences as outlined in the WRSS Student Code of Conduct

Complete and return the following page

Warrigal Road State School

314 Warrigal Road Ph 3340 5333
Eight Mile Plains 4113 Fax 3340 5300
Email address: admin@warrigalroadss.eq.edu.au

Bring Your Own Device (BYOD)
Responsible Use Policy Agreement

I/We have:

- read and understood the *ICT Responsible Use Policy* and the *Bring Your Own Device Program Information and Procedures Handbook.*
- agreed to abide by the above rules.
- been made aware that any breaches of the student's code of conduct may result in disciplinary consequences as per Warrigal Road State School's Student Code of Conduct

Parent/s and student agree to abide by the WRSS **ICT Responsible Use Policy.**

Student's Name: …… **Year Level :** ……

(PLEASE PRINT)

Student's Signature: ……. **Date:** / /

Parent's/Guardian's Name: ……..

(PLEASE PRINT)

Parent's/Guardian's Signature: ……... **Date:** / /