KARALEE STATE SCHOOL
LEARNING TOGETHER

Principal:	Mrs Michelle Hamlin
Deputy Principal:	Mrs Jodie Jones
Business Manager:	Mrs Lynnelle Jones

ABN: 33 324 846 461

BYOD

STUDENT CHARTER

2025

TABLE OF CONTENTS

- Personally-owned Laptop charter 3
  - BYOD overview 4
  - Device selection 5
  - Device care 5
  - Data security and back-ups 6
- Acceptable personal mobile device use 7
  - Passwords 8
  - Digital citizenship 8
  - Cybersafety 9
  - Web filtering 10
  - Privacy and confidentiality 11
  - Intellectual property and copyright 11
  - Software 12
  - Monitoring and reporting 12
  - Misuse and breaches of acceptable usage 12
- Equity Access (Students) 13
- E-Waste Policy 13
- Responsible use of BYOD 14
- Responsible use agreement 17

At Karalee State School we believe that the BYOD program will be successful if the long-term goals listed below remain a priority. The long-term priorities were developed by Staff and Family representatives in 2020.The teachers at Karalee will become pedagogical leaders in digital literacy.

- The students at Karalee will have equitable access to the program.
- The students at Karalee will be taught Cybersafety strategies to ensure that the digital learning platform is a safe space for all students.
- The BYOD Karalee program will incorporate best practice in recycling and e-waste management.
- The school will maintain the highest standards in relation to staff and student data security.
- The school will align the BYOD to the Australian Curriculum to help students transition positively to middle school and beyond.

BYOD OVERVIEW

Bring Your Own Device (BYOD) is an Education Queensland pathway supporting the delivery of 21st century learning. It is a term used to describe a digital device ownership model where students use their personally-owned mobile device to access the department's information and communication (ICT) network.
Access to the department's ICT network is provided only if the mobile device meets the department's security requirements.

Students are responsible for the security, integrity, insurance and maintenance of their personal mobile devices and their private network accounts.

The BYOD acronym used by the department refers to the teaching and learning environment in Queensland state schools where personally-owned mobile devices are used. The department has carried out extensive BYOD research within Queensland state schools. The research built on and acknowledged the distance travelled in implementing 1-to-1 computer to student ratio classes across the state, and other major technology rollouts.

We have chosen to support the implementation of a BYOD model because:

- BYOD recognises the demand for seamless movement between school, work, home and play.
- Our BYOD program assists and supports students to improve their learning outcomes in a contemporary educational setting.
- Our BYOD program assists students to become responsible digital citizens, enhances the teaching learning process and achievement of student outcomes as well as the skills and experiences that will prepare and support their preparation for future studies and careers.
- The BYOD program integrates the use of the ICT General Capabilities from the Australian Curriculum.

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.

The school's BYOD program supports filtered internet access, and file access and storage through the department's network while at school. However, the school's BYOD program does not include school technical support or charging of devices at school.

DEVICE CARE

The student is solely 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.

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.
- Carrying devices with the screen open should be avoided.
- Ensure the battery is fully charged each day.
- Turn the device off before placing it in its bag.

Protecting the 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.

DATA SECURITY AND BACK-UPS

Students must ensure they have a process of **backing up data securely.** Otherwise, should a hardware or software fault occur, assignments and the products of other class activities may be lost.

The student is solely responsible for the backup of all data.

Students are able to backup their device using OneDrive which is provided through Education Queensland using their school account details. Note that this data will be lost when leaving the public school system.

The backup of this data is the sole responsibility of the student and should be backed-up on an external device, such as an external hard drive, USB drive or OneDrive.

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.

Upon enrolment in a Queensland Government school, parental or caregiver permission is sought to give the student(s) access to the internet.

This policy also forms part of this Student Laptop Charter. The acceptable-use conditions apply to the use of the device and internet both on and off the school grounds. Communication through internet and online communication services must also comply with the department's **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.
- participate in any online bullying or data sharing that puts themselves or others at risk.

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 username 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 should be changed when prompted by the department or when known by another user. **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.

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 expectations. The school's Student Code of Conduct also supports students by providing school related expectations, guidelines and consequences.

CYBERSAFTEY

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 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.**

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 Department 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.

INTELLECTUAL PROPERTY AND COPYRIGHT

Students should never plagiarise information and should observe appropriate copyright clearance, including acknowledging the original author or source of any information, images, audio etc. used. It is also important that the student obtain all appropriate permissions before electronically publishing other people's works or drawings. The creator or author of any material published should always be acknowledged. Material being published on the internet or intranet must have the approval of the principal or their delegate and have appropriate copyright clearance.

Copying of software, information, graphics or other data files may violate copyright laws without warning and be subject to prosecution from agencies to enforce such copyrights.

SOFTWARE

Schools may recommend software applications in order to meet the curriculum needs of particular subjects. **Parents/caregivers may be required to install and support the appropriate use of the software in accordance with guidelines provided by the school.** This includes the understanding that software may need to be removed from the device upon the cancellation of student enrolment, transfer or graduation.

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.

Material on the device is subject to audit by 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. Consequences are outlined in the Student Code of Conduct for Karalee State School. 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.**

The whole school community (School and P&C) will endeavour to support families who may be experiencing financial hardship which prevents them from purchasing a BYOD. The school P&C provide funding for the school's ICT improvement agenda annually. Funds from this allocation will be used to support equity of access to the BYOD program.

E-WASTE POLICY (DIGITAL HARDWARE)

Families participating in the BYOD program will be made aware that e-waste options are available for unused or damaged hardware. Members of the school community have access to recycling or reusing programs that will ensure that the Karalee BYOD program doesn't add to the local communities' landfill.

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

RESPONSIBILITIES OF STAKEHOLDERS INVOLVED IN 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 (please consult Technical support table below)
- some school-supplied software e.g. Adobe, Microsoft Office 365
- school representative signing of BYOD Charter Agreement.

STUDENT

- participation in BYOD program induction
- acknowledgement that purpose of device at school is for educational purposes
- care of device
- appropriate digital citizenship and online safety (for more details, visit the website of the Australian eSafety Commissioner)
- only using the camera function with staff permission for a specific purpose
- 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)
- some technical support (please consult Technical support table below)
- 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 BYOD Charter Agreement.

PARENTS AND CAREGIVERS

- participation in BYOD program information session
- 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, visit the website of the Australian eSafety Commissioner)
- some technical support (please consult Technical support table below)
- required software
- protective backpack or case for the device
- adequate warranty and insurance of the device
- understanding and signing the BYOD Charter Agreement.

TECHNICAL SUPPORT

	Connection	Hardware	Software
Parents and Caregivers	(Home-provided internet connection)		
Students			
School	School provided internet		Some school-based software arrangements
Device Vendor		See specifics of warranty purchase	

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

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

However, the school's BYOD program does not support personally-owned mobile devices in regard to:

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

Acknowledgement of the BYOD Charter to be returned to class teacher asap.

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

- I have read and understood the BYOD Charter and the Student Code of Conduct.
- I agree to abide by the guidelines outlined by both documents.
- I am aware that non-compliance or irresponsible behaviour, breaching the intent of the BYOD Charter and the Student Code of Conduct, will result in consequences relative to the behaviour.

Student's Name: ____________________________________ Year Level _____
(Please Print)

Student's signature: ____________________________ Date _____________

Parent's/ Caregiver's Name: _________________________________

Parent's/ Caregiver's signature: ______________________________ Date _____________
(Please Print)

Reference: Student Code of Conduct
https://karaleess.eq.edu.au/SupportAndResources/FormsAndDocuments/Documents/student-code-of-conduct-karalee-state-school.pdf#search=student%20code%20of%20conduct