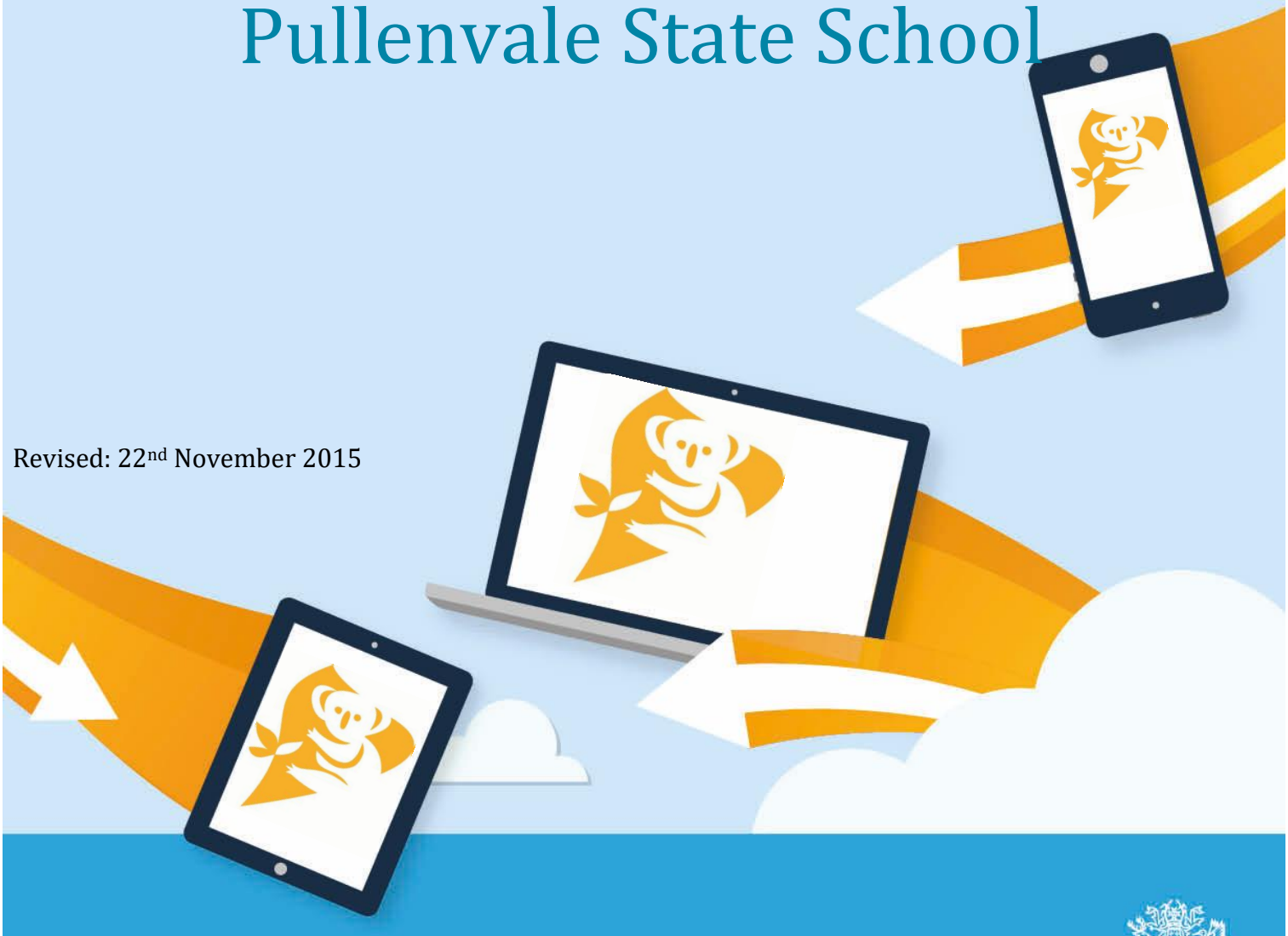
Student ePAL charter

Pullenvale State School



Revised: 22nd November 2015

Contents

Device charter

ePal overview

Electronic Personal Anywhere Learning (ePal) is Pullenvale State School's Bring Your Own Device (BYOD) and Choose Your Own Device (CYOD) program supporting the delivery of 21st century learning.

These mobile devices include but are not limited to laptops, tablet devices and smart phones. Access to the department's ICT network is provided only if the mobile device meets the department's security requirements which, at a minimum, requires that anti-virus software has been installed where possible, is running and is kept updated on the device.

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

We have chosen to support the implementation of ePAL because:

- ePAL recognises the demand for seamless movement between school, work, home and play
- ePAL assists students to improve their learning outcomes in a contemporary educational setting
- assisting 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 them for their future studies and careers.

The school's ePAL program will provide filtered internet access and online storage through the department's network while at school. The online storage will also be available from home. ePAL program does not allow for charging of devices at school.

Device care

The student is responsible for taking care of and securing the device and accessories. 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.

Use of the devices before/after school or during breaks is not permitted without the expressed permission of a teacher and under their direct supervision. Before and after school, the devices are to remain in school bags under the responsibility of the student. Devices will remain in classrooms between 9am-3pm with classrooms being locked whenever the class is out of the classroom or during breaks.

Under no circumstances should devices be left in unsupervised areas.

It is advised that accidental damage and warranty policies are discussed at point of purchase with your retailer 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 responsible for the backup of all data. While at school, students may be able to save data to the school's online virtual classroom called edStudio which is safeguarded by a scheduled backup solution.

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

Parents 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.

Acceptable personal mobile device use

Upon enrolment to Pullenvale State School, parental or caregiver permission is sought to give the student(s) access to the internet, based upon the policy contained within the Responsible Behaviour Plan (available on school website).

This policy also forms part of this Student ePAL Charter. The acceptable-use conditions apply to the use of the device and internet both on and off the school grounds.

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
- intentionally download illegal software or music
- intentionally damage or disable computers, computer systems, school or government networks
- use the device for any unlawful purposes or commercial activities.

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 should be changed regularly, as well as 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 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. E.g. Windows 8.1 provides a “Family Safety” feature.

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.

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 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.

(https://esafety.gov.au/complaints-and-reporting/cybersafety-help-button)

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. (http://behaviour.education.qld.gov.au/cybersafety/Pages/default.aspx)

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. 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 DETE 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 Office of the Children's eSafety Commissioner website (https://esafety.gov.au/) for resources and practical advice to help young people safely enjoy the online world.

Privacy and confidentiality

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.

Software

Pullenvale State School 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.

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 school network 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 in accordance with the school's Responsible Behaviour Plan.

Responsible use within ePAL Program

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 the ePAL program:

School

- ePAL program induction — including information on (but not responsible for) care of device at school, workplace health and safety, appropriate digital citizenship and cybersafety
- network connection at school
- internet filtering (when connected via the school's computer network)
- some technical support (please consult Technical support table below)
- school representative signing of ePAL Charter Agreement.

Student

- participation in ePAL program induction
- acknowledgement that the core purpose of device at school is for educational purposes
- care of device
- appropriate digital citizenship and online safety
- security and password protection
- 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 ePAL Charter Agreement.

Parents and caregivers

- participation in ePAL 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
- some technical support (please consult Technical support table below)
- required software, including sufficient anti-virus software
- protective case for the device
- adequate warranty and insurance of the device
- understanding and signing the ePAL Charter Agreement.
- ensure the student brings the device to school everyday.

- All cases, sleeves and devices are clearly labelled and that devices are charged to sufficiently last for the school day.

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 behaviors
  - authoring text, artwork, audio and visual material for publication for educational purposes as supervised and approved by school staff
  - communicating or collaborating with other students, teachers, parents, caregivers or experts as part of assigned school work
  - accessing online references such as dictionaries, encyclopedias, 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.
- 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 of illegal software, 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
- intentionally damaging any devices, accessories, peripherals, printers or network equipment
- committing plagiarism or violate copyright laws
- sending chain letters or spam email (junk mail)
- 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.

Responsible use agreement

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

- I have read and understood the ePAL Charter and the school Responsible Behaviour Plan.
- I agree to abide by the guidelines outlined by both documents.
- I am aware that non-compliance or irresponsible behavior, as per the intent of the ePAL Charter and the Responsible Behaviour Plan, will result in consequences relative to the behaviour.

Student's name: ..... **Year:** .....
(Please print)

Student's signature: ......**Date:** / /

Parent's/caregiver's name:.....
(Please print)

Parent's/caregiver's signature: .....**Date:** / /