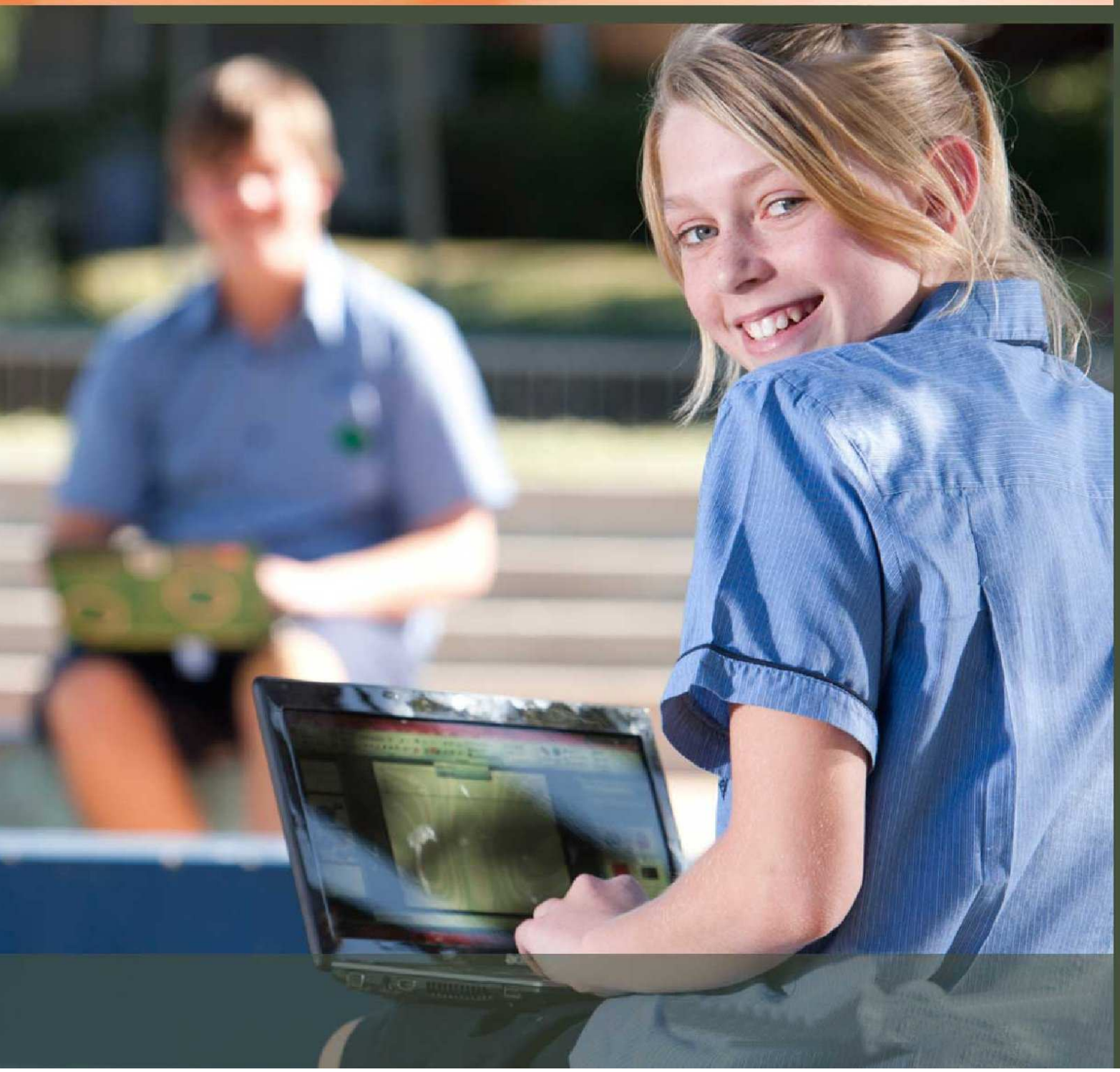
SMART Classrooms

Beaudesert State High School

Bring Your Own Device (BYOx) Charter

2017



DEPARTMENT OF EDUCATION AND TRAINING

Contents

Bring Your Own Device (BYOx) Charter

General Usage

Device adapter

- Do **not** bring your adapter to school as it is easily lost or stolen, and it's use may be hazardous within a school environment.

Battery

- Have a fully charged battery at the start of each school day. All charging should be undertaken at home, as the school will not have the infrastructure or resources available to charge batteries for every student.

Software

- Do not copy any software from the school's ICT network or system (the ONLY exception is eTextbooks, which may be offered to students).
- All technology equipment should only have operating systems loaded that are compliant with departmental standards.
- Keep your virus check software up-to-date. If your virus check software detects virus activity then carefully follow the instructions for removal and advise the School's IT Support Department ***immediately***. If unsure, quarantine your device and ***immediately*** consult with the School's IT Support Department.
- Always adhere to licensing and copying agreements.
- Never use devices to engage in illegal activity, including violation of copyright or other contracts.

Security

- Report any suspected virus activity to the School's IT Support Department.
- Make regular backups of your saved work (this is YOUR responsibility).
- Keep your login and password confidential.
- Do not attempt or undertake any malicious activity towards the school's ICT resources.
- Do not attempt unauthorised access of school ICT resources or entities.

Data security

Students must understand the importance of backing up data securely. Should a hardware or software fault develop, assignment work that has taken a considerable time to prepare may be lost. **The student is responsible for the backup of all their data.** Whilst at school, students are able to save data to the school's network, which is safeguarded by a scheduled backup solution. They should also be able to save data locally to the device for use away from the school network. The backup of this data is the responsibility of the student and this data should be backed-up on an external device, such as external hard drive or USB stick.

Acceptable computer, device and internet use

Upon enrolment in a Queensland Government school, parental or caregiver permission is sought to give the student(s) access to the internet, based upon the policy contained within ICT-PR-004 Using the Department's Corporate ICT Network. http://ppr.det.qld.gov.au/Pages/default.aspx

This policy also forms part of this BYOx Charter. The acceptable use conditions apply to the use of the device and internet.

Communication through internet and online communication services must comply with the Responsible Behaviour Plan available on the school website.

Conditions of Use for Students

1. If you do not comply with these rules contained within this *BYOx Charter*, you will not be allowed to use the device within the school environment. There may be other disciplinary consequences under your school's Responsible Behavior Plan for Students as outlined in *SMS-PR-021: Safe, Supportive and Disciplined School Environment* http://education.qld.gov.au/strategic/eppr/students/smspr021/
2. The s*chool's Student Network / Internet Access Agreement* and *Internet Usage Policy* also apply to your use of the network / internet when you are accessing the internet using the device. You are reminded of your obligations under that agreement and policy.
3. You accept responsibility for the security and care of the device.
4. You are responsible for backing-up all necessary data. The school is not responsible for any data loss. Please ensure all your school work and important documents are backed up onto a USB device.
5. You must ensure that the software provided by the school is not copied, deleted or transferred for any reason at all. Unauthorised use may breach copyright laws.
6. You must take all reasonably necessary steps to prevent a virus from infecting the school network via the device, including monitoring any data that is downloaded or uploaded onto the device from the Internet or any device and virus checking any USB drives in the device.
7. Images or sound captured by personal technology devices on the school premises or elsewhere must not be disseminated to others using the device, for the purpose of causing embarrassment to individuals or the school for the purpose of bullying or harassment, or where without such intent a reasonable person would conclude that such outcomes may occur. The school has the right to invoke appropriate disciplinary processes to deal with such behaviour by a student.
8. You must not intentionally use the device or internet services to which it may be connected:

    - for any illegal, pornographic, fraudulent or defamatory purposes;
    - for transmission of unsolicited electronic mail;
    - to send, or cause to be sent, any computer worms, viruses or other similar programs;
    - to menace or harass another person (or use in a way that would be regarded by a reasonable person to be offensive);
    - to transmit any harassing, obscene, indecent, offensive, or threatening material or emails;
    - to reproduce, distribute, transmit, publish, copy or exploit any material that constitutes an infringement of any intellectual property rights (such as copyright) of a third party; or

- in a way that violates any laws, such as privacy laws.

9. In particular you must not use the device (or any internet services to which it may be connected) to bully, harass or be unkind to other persons.
10. 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 of the school's information technology resources.
11. Students should not use school-provided internet to intentionally download unauthorised software, graphics or music.
12. Students should not intentionally damage or disable computers, computer systems or Queensland DET networks.
13. Students should not use the school-provided internet for unauthorised commercial activities, political lobbying, online gambling or any unlawful purpose.

Note: Students' use of the internet and online communication services, as well as general computer usage, can be audited and traced to the account of the user.

Passwords

School account passwords must not be obvious or easily guessed; they must be kept confidential, and changed when prompted or when known by another user. Personal accounts must not be shared. Students must not allow others to use their personal account for any reason.

In the interest of a secure network, if it is suspected that a personal account has been 'put at risk' (e.g. password known by another person), the personal account will be immediately disabled and not enabled until the risk has been eliminated.

Cybersafety

If the student believes they have received a computer virus or spam (unsolicited email), or if they have received a message that is inappropriate or makes them feel uncomfortable, they must inform their teacher, parent and/or caregiver as soon as is possible.

Students are encouraged to explore and use the 'Cybersafety Help' button to talk about, report and learn about a range of cybersafety issues.

Students must 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 messages, 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 or publish:

- unacceptable or unlawful material or remarks, including offensive, abusive or discriminatory comments.
- threats, bullying or harassing in nature to another person.
- sexually explicit or sexually suggestive material or correspondence.
- false or defamatory information about a person or organisation.

Bluecoat web filtering

Internet filtering protection solutions provide the department with the ability to restrict access to inappropriate material on the department's ICT network.

This covers school web browsing from the department's central servers. Web filtering is also enabled when using Education Queensland accounts to access third party internet access points, such as your internet at home or a council wireless hotspot.

It is important to remember that filtering systems are not foolproof and do not replace the need for parental supervision when students are online. Parents, caregivers and students are encouraged to visit the Cybersmart website at www.cybersmart.gov.au.

Privacy and confidentiality

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.

The student should not reveal personal information, including names, addresses, photographs, credit card details or telephone numbers of themselves or others.

It should also be ensured that privacy and confidentiality is maintained by not disclosing or using any information in a way that is contrary to any individual's interest.

Intellectual property and copyright

Students should never plagiarise information and shall observe appropriate copyright clearance, including acknowledging the original author or source of any information 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.

Misuse and breaches of acceptable usage

Students should be aware that they are held responsible for their actions whilst 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 the internet, network and online communication services.

The misuse of the internet and online communication services may result in disciplinary action, which includes, but is not limited to, the withdrawal of access to services or device.

Software

The parent or caregiver must ensure that the software provided by the school is not copied, deleted or transferred, without prior written consent from the school. Unauthorised use may breach copyright laws and the parent or caregiver may be held liable for any damages incurred.

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.

Remote viewing software may be installed by the school. This software can be utilised to remote-view users' sessions whilst at school.

Students' reporting requirements

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 must also be reported to the school.