STUDENT BRING YOUR OWN DEVICE (BYOD) GUIDELINES

1. Introduction

The *Bring Your Own Device* (BYOD) guidelines contain information for schools that choose to allow student use of personal mobile electronic devices at school to access the NSW Department of Education and Communities' Wi-Fi network.

The term "device" refers to any mobile electronic technology, including assistive technologies, brought into the school, which is owned by the student, and which has the capability of connecting to the department's Wi-Fi network.

2. Research

A literature review undertaken by the NSW Department of Education and Communities in 2013 found that the key considerations for implementing BYOD were:

- The widespread availability of wireless internet-enabled devices.
- The integral nature of these devices to the students' own world.
- The possibility of leveraging students' attachment to their own devices to deepen learning and to make learning more personalised and student-centred.

The review found a range of international implementation models including:

- The "locked down" model where the device and software to be used are dictated and controlled by the school.
- The "specific requirements" model where the student chooses the device, however, it must have specific software or apps, a minimum sized RAM and hard drive.
- The "BYO anything" model, also known as "Bring Your Own Technology (BYOT) model, where schools accept any personally-owned device provided it is internet ready.

The pedagogy that is used in conjunction with the devices is a key factor in determining the model used.

- In a teacher-centred learning environment, the BYOD model should focus on students having the same software and desktop experience, with either a single standard device managed by the school or a controlled range of devices.
- In the student-centred learning environment, far less standardisation and control is required. Some devices (e.g. laptops) are able to carry out more tasks than others. The potential for their use in pedagogy needs to be carefully assessed before decisions are made.

Schools and their communities are best placed to determine the most appropriate BYOD model for their school.

3. Policy requirements

3.1 Schools can allow students to bring devices to school for the purpose of learning.

3.2 Use of devices at school will be governed by school-developed policies.

3.3 Prior to implementing BYOD, schools should provide information to key community stakeholders including teachers, parents, caregivers and students.

3.4 Students and their parents/caregivers must complete and return a signed BYOD Student Agreement prior to participation in BYOD.

3.5 The school and its community can choose the BYOD model that is relevant and appropriate for the needs of the students and the community.

3.6 Prior to implementing BYOD, schools should consider/identify strategies to ensure that all students are able to engage fully in classroom activities. This should include strategies to accommodate students without a device.

4. Access to the department's Wi-Fi network and resources

4.1 Internet access through the department's Wi-Fi network will be provided on departmental sites at no cost to students who are enrolled in NSW public schools.

4.2 Access to school resources such as shared drives, printers and associated costs will be a school-based decision.

5. Acceptable use of devices

The principal will retain the right to determine what is, and is not, appropriate use of devices at the school within the bounds of the department's policies and NSW privacy and other legislation.

Schools should review existing policies and processes to include the BYOD policy, where appropriate.

5.1 Students must comply with departmental and school policies concerning the use of devices at school while connected to the department's Wi-Fi network.

5.2 Mobile phone voice and text, SMS messaging or device instant messaging use by students during school hours is a school-based decision.

5.3 Students should not attach any school-owned equipment to their mobile devices without the permission of the school principal or an appropriate staff member.

5.4 Students must not create, transmit, retransmit or participate in the circulation of content on their devices that attempts to undermine, hack or bypass any hardware and software security mechanisms that have been implemented by the department, its Information Technology Directorate or the school.

5.5 Students must not copy, transmit or retransmit any material that is protected by copyright, without prior permission from the copyright owner.

5.6 Students must not take photos or make video or audio recordings of any individual or group without the express written permission of each individual (including parent/caregiver consent for minors) being recorded and the permission of an appropriate staff member.

5.7 Students must not use the department's network services to seek out, access, store or send any material of an offensive, obscene, pornographic, threatening, abusive or defamatory nature is prohibited. Such use may result in disciplinary and/or legal action.

5.8 Students and their parents/caregivers must be advised that activity on the internet is recorded and that these records may be used in investigations, court proceedings or for other legal reasons.

Where a school has reasonable grounds to suspect that a device contains data which breaches the BYOD Student Agreement, the principal may confiscate the device for the purpose of confirming the existence of the material. Depending on the nature of the material involved, school disciplinary action may be appropriate or further action may be taken including referral to the police.

The consequences of any breaches of the school's BYOD policy will be determined by the principal in accordance with relevant Department policies and procedures and accepted school practice

6. BYOD Student Agreement

Schools must ensure that students and their parents/caregivers are aware of, and agree to their obligations under the school's BYOD policy and other relevant departmental policies.

6.1 Prior to connecting their devices to the department's Wi-Fi network, students must return a BYOD Student Agreement.

6.2 The BYOD Student Agreement contains both BYOD Device Requirements and BYOD Student Responsibilities.

6.3 The BYOD Student Agreement must be signed by the student and by a parent/caregiver. If a student is living independently of their parents/caregivers or is 18 years of age or more, there is no requirement to obtain the signature of a parent/caregiver. Principals will make these determinations.

6.4 By accepting the terms of the BYOD Student Agreement, the student and parents/caregivers acknowledge that the student:

- agrees to comply with the conditions of the school's BYOD policy; and
- understands that noncompliance may result in disciplinary action.

Schools should retain a copy of the BYOD Student Agreement in print or electronic form and it should be kept on file with the student record.

7. Long-term care and support of devices

Students and their parents/caregivers are solely responsible for the care and maintenance of their devices.

7.1 Students must have a supported operating system and current antivirus software, if applicable, installed on their device and must continue to maintain the latest service packs, updates and antivirus definitions.

7.2 Students are responsible for ensuring the operating system and all software on their device is legally and appropriately licensed.

7.3 Students are responsible for managing the battery life of their device. Students should ensure that their devices are fully charged before bringing them to school. Schools are not responsible for providing facilities for students to charge their devices.

7.4 Students are responsible for securing and protecting their device in schools, and while travelling to and from school. This includes protective/carry cases and exercising common sense when storing the device. Schools are not required to provide designated or secure storage locations.

7.5 Students should clearly label their device for identification purposes. Labels should not be easily removable.

7.6 Students should understand the limitations of the manufacturer's warranty on their devices, both in duration and in coverage.

8. Damage and loss

8.1 Students bring their devices onto the school site at their own risk.

8.2 In cases of malicious damage or theft of another student's device, existing school processes for damage to school or another student's property apply.

9. Technical support

Schools are under no obligation to provide technical support for hardware or software. Colo High School has a Technical Support Officer who can provide basic support services to ensure a device can operate within the BYOD program.

10. Insurance

Student devices are not covered by Treasury Managed Fund. Insurance is the responsibility of parents/caregivers and students. It is recommended that families seek their own insurance or warranty plans when seeking a device to purchase.

11. Device requirements

The BYOD Device Requirements' document and the BYOD Student Responsibilities' document has been developed and contains information relating to:

- Departmental technology standards
- Hardware specifications, including the operating system
- Student responsibilities relating to the BYOD program.

12. Security and device management processes

Depending on the model of BYOD a school chooses, the following considerations are essential:

- strong passwords (the portal has Password Help information);
- device anti-virus software (if applicable) and privacy controls.

The department's Digital Citizenship (www.digitalcitizenship.nsw.edu.au) website contains information to support security and device management.