TEVEN-TINTENBAR PUBLIC SCHOOL

BRING YOUR OWN DEVICE (BYOD) GUIDELINES

1. Introduction

The Bring Your Own Device (BYOD) guidelines contain information about 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 and laptops, 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.

3. Policy requirements

3.1 Students in Years 4-6 are allowed 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 Students and their parents/caregivers must complete and return a signed BYOD Student Agreement prior to participation in BYOD.

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.
4.2 Access to school resources such as shared drives, printers will be provided on departmental sites at no cost to students.

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.

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 not allowed.
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 are 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 the 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

The school will 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.

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.

The school will retain a copy of the BYOD Student Agreement in print or electronic form which will 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 as outlined on the BYOD Student Responsibilities document.

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. The school is not responsible for (or restricted from) 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. The school is 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

The school is under no obligation to provide technical support for hardware or software.

10. Insurance

Student devices are not covered by Treasury Managed Fund. Insurance is the responsibility of parents/caregivers and students.

11. DEC technology standards

Students should be aware of the following essential information regarding technology standards for devices used within schools.

11.1 The department's Wi-Fi network installed in our school operates on the 802.11n 5Ghz standard. Devices that do not support this standard will not be able to connect.

12. Device requirements

Devices that can be used through the BYOD must meet the following requirements:

12.1 The smallest size allowable is that of an IPad mini or Kindle. IPod touches, IPhones or similar devices are not permitted under our BYOD policy.

12.2 Devices should have the Mathletics App installed.

12.3 All Apps that can be opened by student must be G rated (under 12, no violence or swearing). If a device holds PG, M or R rated Apps or data, these need to be in a file that has a parental lock installed or altogether removed from the device.

12.4 Devices MUST not be held on students' laps. They are to be on a desk, on the floor or hand held for short periods.

12.5 Students are not to download APPS at school unless requested by their teacher.

13. Security and device management processes

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