SMITHFIELD PUBLIC SCHOOL

Strive For the Best

Student Bring Your Own Device (BYOD) Policy

This policy provides direction to schools choosing to allow student use of personal mobile electronic devices at school to access the Department of Education and Communities' wireless network.

1 Objectives – Policy Statement

1.1 The term "device" in this policy refers to any personal mobile electronic device with the capability to connect to the department's Wi-Fi network.
1.2 Schools can allow students to bring their own devices to school and may provide access to the department's Wi-Fi network.
1.3 Use of devices at school will be governed by school developed guidelines and processes based on the Bring Your Own Device Implementation Guidelines
1.4 The department will provide internet access through its wireless networks at no cost to students enrolled in NSW Public Schools at DEC sites.
1.5 Students are responsible for the care and maintenance of their devices including data protection and battery charging.
1.6 The department will not accept any liability for the theft, damage or loss of any student's device. Students who bring their own devices onto school sites do so at their own risk.
1.7 Schools are not obliged to provide hardware or technical support for devices.
1.8 Students and their parents/carers must complete and return a signed BYOD Agreement prior to connecting to the department's Wi-Fi network.
1.9 Where the school has reasonable grounds to suspect that a device contains data which breaches the BYOD Agreement, they may confiscate the device for the purpose of confirming the existence of the material. Depending on the nature of the material involved, further action may be taken including referral to the police. School disciplinary action may also be appropriate.

2 Audience and applicability

2.1 This policy applies to students connecting a device to the department's Wi-Fi network.

3 Context

3.1 The increasing availability of personal technology has accelerated the demand for new models of learning, whereby students may be encouraged to bring their own devices to school.

3.2 Choosing to implement BYOD access can provide a process to allow schools and the department to efficiently incorporate student-owned devices into our digital learning environments while protecting school and DEC infrastructure and data.

3.3 This policy should be read and interpreted in conjunction with:
● Code of Conduct Policy
● Values in NSW Public Schools
● DEC Privacy Code of Practice
● Online Communication Services – Acceptable Usage for school students
● Legal Issues Bulletin No. 35 November 2012 – Use of mobile phones, portable computer games, recording devices and cameras in schools
● Legal Issues Bulletin No. 8 September 2012 – Claims for loss of or damage to personal property
● Smartcopying – Copyright guide for schools.

3.4 Document history and details (to be left in bold)

4 Responsibilities and Delegations

4.1 *Principals* are responsible for the implementation of this policy and guidelines in their school and are required to ensure that this policy is followed by participating *students* and their *parents/carers*.

4.2 *Principals* are responsible for dealing with any breach of the BYOD Agreement as outlined in the Bring Your Own Device Implementation Guidelines.

4.3 *The department* conducts surveillance and monitoring of its computer systems to ensure the ongoing confidentiality, integrity and availability of services.

5 Monitoring, evaluation and reporting requirements

5.1 Principals will supervise the implementation of the policy and report their evaluations to their Director, Public Schools NSW.

5.2 ITD will update this policy and the guidelines referenced as technologies change or as required.

NSW DEC Bring Your Own Device Student Agreement

Students who wish to take advantage of the BYOD policy must read this agreement in the company of an adult unless otherwise excused by the principal. This page is to be signed and returned to the school. By signing at the bottom of this page students agree to the following behaviours:

❒ I agree that my use of the department's internet will be *primarily for learning*.

❒ I agree to only *ever use my own portal/internet log-in* details and never share those with others.

❒ I agree to not *hack* or *bypass any hardware and software security* implemented by the Department or my school.

❒ I agree to not use BYOD to knowingly *search* for, *link* to, *access* or *send* anything that is;

- offensive
- inappropriate
- threatening
- abusive
- defamatory

❒ I agree to *report inappropriate behaviour* and material to my teacher.

❒ I agree to stay safe by *not giving out my personal information* to strangers.

❒ I understand that *my activity on the internet is recorded* and these records may be used in investigations, court proceedings or for other legal reasons.

❒ I acknowledge that the *school cannot be held responsible* for any *damage* to or *theft* of my device.

❒ I agree to store my device/s in the classroom storeroom during Lunch and Recess.

❒ I agree that use of my device during school activities is at the *direction of the teacher*.

Date: ___/___/____

_____ in the presence of: _____

Student Name *Parent/Carer Name*

_____ in the presence of: _____

Student Signature *Parent/Carer Signature*

NSW GOVERNMENT Education & Communities

Student Agreement Appendix – Detailed information for parents

Online Communication Services: Acceptable Usage for School Students

Responsibilities and delegations

Access and Security

Students will:

☐ ensure that communication through internet and online communication services is related primarily to learning.

☐ keep passwords confidential, and change them when prompted, or when known by another user.

☐ use passwords that are not obvious or easily guessed.

☐ never allow others to use their personal e-learning account.

☐ log off at the end of each session to ensure that nobody else can use their e-learning account.

☐ promptly tell their supervising teacher if they suspect they have received a computer virus or spam (i.e. unsolicited email) or if they receive a message that is inappropriate or makes them feel uncomfortable.

☐ seek advice if another user seeks excessive personal information, asks to be telephoned, offers gifts by email or wants to meet a student.

☐ never knowingly initiate or forward emails or other messages containing:

- a message that was sent to them in confidence.
- a computer virus or attachment that is capable of damaging recipients' computers.
- chain letters and hoax emails.
- spam, e.g. unsolicited advertising material.

☐ never send or publish:

- unacceptable or unlawful material or remarks, including offensive, abusive or discriminatory comments.
- threatening, bullying or harassing another person or making excessive or unreasonable demands upon another person.
- sexually explicit or sexually suggestive material or correspondence.
- false or defamatory information about a person or organisation.

☐ ensure that personal use is kept to a minimum and internet and online communication services is primarily used for genuine curriculum and educational activities. Use of unauthorised programs and intentionally downloading unauthorised software, graphics or music that is not associated with learning, is not permitted.

☐ ensure that services are not used for unauthorised commercial activities, political lobbying, online gambling or any unlawful purpose.

☐ be aware that all use of internet and online communication services can be audited and traced to the e-learning accounts of specific users.

Responsibility for device

Students should be aware that:

☐ the school accepts no responsibility for the theft, damage or loss of any device a student brings onto the school site

☐ they bring their devices onto the school site at their own risk

Privacy and Confidentiality

Students will:

☐ never publish or disclose the email address of a staff member or student without that person's explicit permission.

☐ not reveal personal information including names, addresses, photographs, credit card details and telephone numbers of themselves or others.

☐ ensure privacy and confidentiality is maintained by not disclosing or using any information in a way that is contrary to any individual's interests.

Intellectual Property and Copyright

Students will:

☐ never plagiarise information and will observe appropriate copyright clearance, including acknowledging the author or source of any information used.

☐ ensure that permission is gained before electronically publishing users' works or drawings. Always acknowledge the creator or author of any material published.

☐ ensure any material published on the internet or intranet has the approval of the principal or their delegate and has appropriate copyright clearance.

Misuse and Breaches of Acceptable Usage

Students will be aware that:

☐ they are held responsible for their actions while using internet and online communication services.

☐ they are held responsible for any breaches caused by them allowing any other person to use their e-learning account to access internet and online communication services.

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

☐ If they are found with any inappropriate material on their device in breach of the agreement, the device may be confiscated and the matter reported to the police.

Monitoring, evaluation and reporting requirements

Students will report:

☐ any internet site accessed that is considered inappropriate.

☐ any suspected technical security breach involving users from other schools, TAFEs, or from outside the NSW Department of Education and Communities.

Students should be aware that:

☐ their emails are archived and their web browsing is logged. The records are kept for two years.

☐ the email archive and web browsing logs are considered official documents.

☐ they need to be careful about putting their personal or sensitive information in emails or on websites.

☐ these records may be used in investigations, court proceedings or for other legal reasons.

STUDENT BRING YOUR OWN DEVICE (BYOD) POLICY GUIDELINES

1. Introduction

This document provides advice and direction to schools choosing to allow student use of personal mobile electronic devices at school to access the Department of Education and Communities' wireless network.

1.1 The term "device" in this policy refers to any personal mobile electronic device with the capability to connect to the department's Wi-Fi network.

1.2 Schools can allow students to bring their own devices to school and may provide access to the department's Wi-Fi network.

1.3 Use of devices at school will be governed by school developed guidelines and processes based on the Bring Your Own Device Implementation Guidelines and the needs of the school.

1.4 The department will provide internet access through its wireless networks at no cost to students enrolled in NSW Public Schools at DEC sites.

1.5 Students are responsible for the care and maintenance of their devices including data protection and battery charging.

1.6 The department will not accept any liability for the theft, damage or loss of any student's device. Students who bring their own devices onto school sites do so at their own risk.

1.7 Schools are not obliged to provide hardware or technical support for devices.

1.8 Students and their parents/carers must complete and return a signed BYOD Agreement prior to connecting to the department's network.

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

2. Student BYOD Agreement

2.1 Prior to connecting their devices to the network, students must return a Student BYOD Agreement. A sample is provided which schools are able to modify to suit their BYOD model. This agreement must be signed by the student and by a parent/carer. If a student is living independently of their parents or is 18 years of age or more, there is no requirement to obtain the signature of a parent.

2.2 It is important to ensure that students are aware of and agree to their obligations under the Student Bring Your Own Device (BYOD) Policy and relevant policies, prior to using their own device on the DEC Wi-Fi network. School staff should endeavour to ensure that the BYOD student responsibilities are clearly understood by both students and their parents or carers.

2.3 The Student BYOD Agreement is a simple document with the purpose of acknowledging acceptance and agreement of the terms associated with the school's implementation of the Student Bring Your Own Device (BYOD) Policy by both students and parents/carers. It is accompanied by an Information Sheet that must be provided in conjunction with the Student BYOD Agreement.

2.4 By accepting the terms, the student and parents/carers acknowledge that they:

☐ agree to comply with the conditions of the Student BYOD Policy.

☐ understand that noncompliance may result in the student being subject to school disciplinary action.

2.5 Student BYOD agreements should be retained in print or electronic form for future access as required.

3. Cost to Students

3.1 Internet access through the Department's network will be provided at no cost to students enrolled in NSW Public Schools at DEC sites.

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

4. Student Responsibilities

4.1 Students are solely responsible for the care and maintenance of their BYO devices. This includes but is not limited to:

☐ Managing battery life and regular charging of their device.

☐ Labeling their device for identification purposes.

☐ Purchasing and using device protective casing.

☐ Ensuring the device is safe and secure during travel to and from school and throughout the school day.

☐ Maintaining up-to-date anti-virus software and operating system on their device.

☐ Taking insurance coverage of their own device to protect any accidental damage, theft or loss.

4.2 Students are responsible for managing the battery life of their device and acknowledge that the school is not responsible for charging their devices. Students should ensure that their devices are fully charged before bringing them to school. Schools are not responsible for (or restricted from) providing facilities for students to charge their devices.

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

4.4 Students should not attach any school-owned equipment to their mobile devices without the permission of the school principal or their delegate.

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

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

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

5. Damage and loss

5.1 Students bring their devices onto the school site at their own risk. For advice on theft or damage of students personal devices refer to legal issue bulletins below:
☐
https://detwww.det.nsw.edu.au/media/downloads/directoratesaz/legalservices/ls/legalissuesbul/bulletin35.pdf

☐
https://detwww.det.nsw.edu.au/media/downloads/directoratesaz/legalservices/ls/legalissuesbul/bulletin8.pdf

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

5.3 Schools should regularly review existing policies and processes to include BYO devices where appropriate e.g. Student Welfare and Fair Discipline Code.

Technical Support
5.4 NSW DEC staff are under no obligation to provide any technical support on either hardware or software.

6. Long-term care and support of BYODs

6.1 Students are solely responsible for repair and maintenance of their own device. It is not the school's responsibility.

6.2 Warranties: Students should understand the limitations of the manufacturer's warranty on their BYO devices, both in duration and in coverage. Under Australian consumer legislation, warranties usually last for one year, during which any manufacturing defects will be repaired or the device will be replaced (as per the specific terms and conditions of the manufacturer).

6.3 Extended Warranties: At the time of purchase, students may also purchase an optional extended warranty (past the standard warranty period) from the supplier/manufacturer of their device, during which any manufacturing defects that may occur will also be repaired.

7. Insurance

7.1 Student BYO devices are not covered by Treasury Managed Fund. When students purchase their BYO device, they may also purchase an optional insurance policy from the supplier of their device or a relevant insurance company. As mobile devices are subject to a higher risk of accidental damage, prior to signing up for an insurance policy, students should be fully aware of the details and limitations of the policy, including any excess charged for making a claim, and the name of the company that holds the policy. As a guide, a suitable BYOD device insurance policy should cover all types of BYOD devices and provide worldwide, replacement cost coverage against:

☐ accidental damage,
☐ damage from falls and liquids,
☐ theft
☐ fire
☐ vandalism
☐ natural disasters (such as floods, cyclones, earthquakes, tornados, water damage, and power surge due to lightning)

Acceptable use of BYO devices

7.2 Using the DEC 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 legal and/or disciplinary action.

7.3 Students shall 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.

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

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

7.6 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/carer consent for minors) being recorded and the permission of an appropriate staff member.

7.7 Students shall comply with departmental or school policies concerning the use of BYODs at school and while connected to the Department's network including:

☐ Online Communication Services – Acceptable Usage for School Students.

7.8 The principal retains the right to determine what is, and is not, appropriate use of BYODs device at the school within the bounds of NSW privacy and other legislation.

7.9 The consequences of any breaches of this policy will be determined by the principal, in accordance with the school's welfare and discipline policies. As the student device is intended as a *personal learning tool* schools are encouraged to consider a variety of alternatives to ensure equitable access to continued learning opportunities.

8. DEC Technology Standards (This will need to be adjusted to reflect the BYOD model chosen by your school community, a sample is below using the "Bring your own whatever connects to the internet" model identified by Dixon and Tiernay in the literature review)

8.1 Prior to purchasing or using an already purchased device, parents and students should be made aware of the following technology standards required for devices used within schools:

☐ The DEC wireless network installed in **primary schools** operates on the 802.11n **5Ghz** standard. Devices with 802.11a/b/g or 802.11n 2.4Ghz only will not be able to connect.

☐ The DEC wireless network installed in **high schools** only operates on the 802.11n **5Ghz** standard. Devices with 802.11a/b/g or 802.11n 2.4Ghz only will not be able to connect.

☐ The battery life of the device should be capable of lasting 5 hours minimum of constant use without charge.

☐ Device hardware specifications must meet the minimum (ideally the recommended) specifications of the operating system and all applications.

☐ Currently supported Operating System.

8.2 Other considerations when purchasing a device include:

☐ Extended warranty

☐ Device insurance

☐ Protective casing (scratch/impact/liquid-splash resistant)

☐ Additional or spare battery packs

☐ Ergonomics (is this device comfortable to use for an entire school day)

☐ Backup storage such as portable hard drive or USB flash drive

9. Security and device management processes

Depending on the model of BYOD your school chooses, you will need to consider how the following will be implemented:

☐ Strong passwords (your portal has Password Help information),

☐ Device anti-virus software

☐ Data and network traffic encryption

☐ Privacy controls

☐ Internet filtering

☐ DEC technology infrastructure security

☐ Student Cyber Safety