1. **Introduction**

This document provides guidance and direction to principals, staff and school communities for the management of the Student Bring Your Own Device (BYOD) Policy.

2. **Key principles**

   2.1 Access to the Department of Education and Communities (DEC) network, including the Internet, will be made available to students who bring their own devices to school for appropriate learning activities in addition to accessing resources and research materials.

   2.2 BYOD provides an effective process that allows schools and the DEC to efficiently incorporate student-owned devices into our digital learning environment while securing and protecting school and DEC infrastructure and data. BYOD provides an effective process that allows schools and the DEC to efficiently incorporate student-owned devices into our digital learning environment while securing and protecting school and DEC infrastructure and data.

   2.3 Implementation of the Bring Your Own Device (BYOD) Policy is the decision of the individual school. Schools that choose to implement the BYOD policy may develop alternate school specific BYOD solutions so long as these remain within the requirements of the Student BYOD policy and related DEC policies.

   2.4 The device in BYOD refers to any of the following technologies.
   - Laptops
   - Tablets
   - Mobile/smart phones
   - Touch screen devices with WIFI capacity
   - Devices such as PlayStation Portable (PSP) and Nintendo DS are capable of connecting to WiFi however these devices are primarily used for video games and it may be difficult to achieve anticipated learning outcomes.

   2.5 The purpose of this document is to provide an effective process that allows schools and the DEC to efficiently incorporate student-owned devices into our digital learning environment while securing and protecting school and DEC infrastructure and data.

3. **Registration for network accessibility**

   3.1 The school and DEC network will enable student devices in schools and provide a common platform for DEC to engage and ensure device compliance.
4. Student BYOD Agreement

4.1 Prior to connecting their devices to the network, students must return a Student BYOD Agreement. This agreement must be signed by the student and by a parent/carer. The principal may accept the student’s signature for students living independently.

4.2 It is important to ensure that students are aware of and agree to their obligations under the Student Bring Your Own Device (BYOD) Policy prior to using their own device in the school’s digital learning environment. School staff should endeavor to ensure that the BYOD student responsibilities are clearly understood by both students and their parents or carers.

4.3 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.

4.4 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 both the school and the DEC have the capacity to access their device and the data/information it contains at the principal’s discretion.
- Understand that under no circumstances will the DEC or the school accept any liability for the theft, damage or loss of any student’s device.
- understand that non-compliance may result in the withdrawal of BYOD permission and access.

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

5. Cost to Students

5.1 Internet access through the Department’s network will be provided at no cost to students in NSW Public Schools.

5.2 Access to school resources such as printer and its associated costs will be a school-based decision.

6. Student Responsibilities

6.1 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 own device.
- Labeling their own device for identification purposes.
- Purchasing and using device protective casing.
- Ensuring the device is safe and secure.
- 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 or theft or loss.

6.2 Students are responsible for managing the battery life of their BYODs 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 providing facility for students to charge their devices at school.

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

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

6.5 Students should clearly label their BYOD device for identification purposes.

6.6 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.

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

7. **Damage and loss**

7.1 Under no circumstances will the DEC or the school accept any liability for the theft, damage or loss of any student’s device. Please refer to:


7.2 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.

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

8. **Damage and loss**

8.1 Students will not receive any ICT hardware or software technical support from the school, regional ICT support staff or from the NSW DEC for their BYO device.

9. **Long-term care and support of BYODs**

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

9.2 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).

9.3 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.
10. Insurance

10.1 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)

11. Acceptable use of BYO devices

11.1 Using the Department’s 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.

11.2 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 DEC or the school.

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

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

11.5 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.

11.6 Students shall comply with departmental DEC or school policies concerning their use of BYODs device at school and while connected to the Department’s DEC network including:
- Online Communication Services – Acceptable Usage for School Students.
- Acceptable Use of Department’s DEC portal services.

11.7 The principal retains the right to be the final arbiter of what is, and is not, appropriate use of BYODs device at the school within the bounds of NSW privacy legislation.

11.8 The consequences of any breaches of this policy will be determined by the principal, in accordance with the school’s Behaviour and Fair Discipline Policy.
12. DEC Technology Standards

12.1 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

12.2 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

13. Security and device management processes

13.1 The network will become the point where DEC security policies are implemented.

13.2 There are a wide range of security considerations that will be addressed. These include but are not limited to:

- Strong passwords
- Device anti-virus software
- Data and network traffic encryption
- Privacy controls
- Internet filtering
- DEC antivirus
- DEC technology infrastructure security
- Student Cyber Safety

13.3 Educational policies and security processes will be updated as required to ensure a secure and effective digital learning environment.

Developed November 2013
Update Nov 2014
To be redeveloped during 2015