 **Canterbury Public School**

 **Student Bring Your Own Device (BYOD) Policy**

**Rationale**

In the changing educational environment, schools are finding it ever more difficult to develop and maintain modern ICT (Information, Communication and Technology) infrastructure within the current supply model. At Canterbury Public School we believe that students need to be exposed to technology in a comprehensive and integrated manner.

In order to achieve these ends we are implementing this programme to allow students to bring devices to school to enable them to use the latest technology. It will enable staff to teach students with knowledge that all students will have access to this technology and an understanding that they will still have access to the infrastructure already in place.

**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, or remotely to the internet.

1.2 Students will be allowed to bring in devices that can access the DEC wireless service.

1.3 Use of devices at school will be overseen by teachers and the principal in reference to the BYOD 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 wholly responsible for the care and maintenance of their devices including data protection and battery charging. The School and the Department are not obliged to provide technical support for student’s devices.

1.6 Students bring the device to school in the knowledge that it is at their own risk. The School and The department will not accept any liability for the theft, damage or loss of any student’s device at school.

1.7 Before students use their device to access the DEC wireless network they and their parents/caregiver must read and sign the BYOD Agreement.

1.8 If a student uses there device to access or distribute inappropriate or offensive material then the device may be confiscated. The device may be held until a parent/caregiver comes to claim the device. Depending on the nature of material accessed or sent the police may be called. Students may also be subject to school disciplinary action.

1.9 If it believed that a device may contain inappropriate or offensive material then the device may be confiscated to ascertain if such material is present. If the material is present then the device will be held until a parent/caregiver comes to claim the device. Depending on the material contained the police may be called. Students may also be subject to school disciplinary action.

**2 Audience and applicability**

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

2.2 This policy applies to all staff involved with students bringing a device to connect the department’s Wi-Fi network.

2.3 This policy applies to the parents/carers of any student bringing a device to connect 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](https://www.det.nsw.edu.au/policies/staff/ethical_behav/conduct/PD20040020.shtml?query=code+of+conduct)

● [Values in NSW Public Schools](https://www.det.nsw.edu.au/policies/student_serv/student_welfare/valu_scool/pd_05131_Values.pdf)

● [DEC Privacy Code of Practice](https://www.det.nsw.edu.au/privacy/pcp.htm/)

● [Online Communication Services – Acceptable Usage for school students](https://www.det.nsw.edu.au/policies/general_man/general/accep_use/PD20020046.shtml)

● [Legal Issues Bulletin No. 35 November 2012](https://edit.pws.det.nsw.edu.au/documents/27841848/27848137/Legal%20Issues%20bulletin35.pdf) – Use of mobile phones, portable computer games, recording devices and cameras in schools

● [Legal Issues Bulletin No. 8 September 2012](https://www.det.nsw.edu.au/media/downloads/about-us/how-we-operate/legal-issues-bulletins/number_08.pdf) – Claims for loss of or damage to personal property

● [Smartcopying](http://www.smartcopying.edu.au/) – Copyright guide for schools.

**3.4 Document history and details**

**Implementation date:**

**Approval date:**

**Approving Officer:**

**4 Responsibilities**

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 BYOD Implementation Guidelines.

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

4.5 *Parents/carers* are responsible for supporting their children to adhere to the BYOD Implementation Guidelines.

4.5 *Students* are responsible for ensuring that they adhere to the BYOD Implementation Guidelines.

**5 Monitoring, evaluation and reporting requirements**

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

5.2 The school will be responsible for updating this policy as technology and state policy changes dictate. The school will also update this policy in line with changes within the schools context.

5.2 ITD (Information Technology Directorate) will update their policy and the guidelines referenced as technologies change or as required.