CONNELLS POINT PUBLIC SCHOOL
USE OF DIGITAL DEVICES AND ONLINE SERVICES AT SCHOOL

General

Connells Point Public School (the **School**) allows students to bring their own laptop to school and provides access to the Department's Wi-Fi network.

The Department will provide filtered and monitored internet access through its wireless networks at no cost to students on site in NSW Public Schools.

Students are responsible for the care and maintenance of their laptop, including data protection and battery charging. **Students are also required to sign the Code of Conduct.**

The School will not accept any liability for the theft, damage or loss of any student's laptop (intentional or accidental). Students who bring their own laptop to school do so at their own risk. The School is not obliged to provide hardware, software or technical support for laptops.

Responsibilities of parents and carers

The School requires parents and carers to:

- recognise the role they play in educating their children and modelling the behaviours that underpin the safe, responsible and respectful use of digital devices and online services
- support implementation of the school procedure, including its approach to resolving issues
- take responsibility for their child's use of digital devices and online services at home
- communicate with school staff and the school community respectfully and collaboratively.

Parents and carers are to familiarise themselves with the Department's expectations of students using digital devices and online services at school (**attachment 1**), and sign where indicated.

Attachment 1:

The following information outlines appropriate and acceptable use of internet and online communication services provided by the Department of Education (DoE) in a specific school context. For more information visit the DoE's **Student use of Digital Devices and Online Services**.

Access and Security

Students will:

- **not** hack, manipulate or modify settings, attempt to gain access to and/or gain access to password protected content or services
- **not** disable settings for virus protection, spam and filtering that have been applied as a departmental standard
- **not** save, upload, manipulate, transmit or in any other way interact with an image of a student, staff member or community member without the expressed written permission of that individual

- **never** utilise a Virtual Private Network (VPN) or similar communication technology or service to bypass DoE firewalls, filters or safety settings for any purpose
- **never** damage or disable computers, computer systems or networks of the DoE
- **ensure** that communication through internet and online communication services is related to learning
- **never** allow others to use their personal e-learning account
- **not** knowingly damage hardware devices, peripheral devices or networking infrastructure of the school
- **not** upload, download, transmit, save, copy, distribute or print digital content not specifically mapped to a school's teaching and learning or extracurricular program. This includes but is not limited to computer games, applications and system related files, movies, music, images, animations and software intended for monitoring, system related modification, creating aliases or system harm
- **not** utilise school hardware, software, networking infrastructure and related DoE systems for any activity or process not strictly linked to a school teaching and learning or extracurricular program

Students will never send or publish:

- unacceptable or unlawful material or remarks, including offensive, abusive or discriminatory comments
- material that is 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

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

Impersonating, using or creating system users is a serious breach of the Department of Education's Code of Conduct. Students utilising Bring Your Own Device (BYOD) technologies are responsible for abiding by the School's Technology Code of Conduct.

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, this includes all hardware, software and network infrastructure connected to or associated with the school's technology network

Parent/carer name: ……

Parent/carer signature: ……

Date: ……