

Students who wish to take advantage of the BYOD at Canterbury Public School must read this agreement in the company of a guardian. 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 the *primary use* of my device and the departments internet will be for educational use

I agree to only *ever use my own portal/internet log-in* details.

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, material and any breaches* of the BYOD agreement to my teacher.

I agree to stay safe by *not giving out my login details or personal information* to anyone.

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 class storeroom during Lunch, Recess and shall be taken home at the end of each day.

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*

*Student Agreement Appendix – Detailed information for parents*

Online Communication Services: Acceptable Usage for School Students

**https://www.det.nsw.edu.au/policies/general\_man/general/accep\_use/PD20020046.shtml**

**Responsibilities and delegations**

 **Access and Security**

Students will:

* not disable settings for virus protection, spam and filtering that have been applied as a departmental standard.
* ensure that communication through internet and online communication services is related 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 generally 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.
* never damage or disable computers, computer systems or networks of the NSW Department of Education and Training.
* 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.

**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.

**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.

**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