

Woonona High School Bring Your Own Device (BYOD).
YEAR 7 2017 LAPTOP USER CHARTER

Student name _____
Family name _____ Given name _____

Parent/Carer name _____
Family name _____ Given name _____

Purpose

Bring your own device is a new policy and a new way of implementing Technology and Digital Learning at Woonona High School.

As part of this program students will need to purchase a laptop device for school use. This device must meet the requirements set by Woonona High School in order to work properly with the wireless network infrastructure at the school.

Students are expected to make good decisions with regard to their personal use of Technology.

A Laptop User Charter must be signed and provided to Woonona High School before they will be allowed to bring a device to school.

Students and parents/carers must carefully read this charter prior to signing it. Any questions should be addressed to the school and clarification obtained before the charter is signed.

Laptop User Charter

We have read the BYOD User Charter

We understand our responsibilities regarding the use of the laptop and the internet.

In signing below, we acknowledge that we understand and agree to the Laptop User Charter.

We accept that the school is not responsible for BYOD devices. Students are responsible for maintaining the device in working order so they can use it during class. The school takes no responsibility for damage caused to the device within school grounds as well as loss and/or theft of BYOD devices. It is up to the student to keep the device safe.

Signature of student: _____ date: / /

Signature of parent/carers: _____ date: / /

PLEASE SIGN AND RETURN THIS PAGE TO THE SCHOOL

Using a BYOD device.

1. The student is responsible for:

- a. Bringing the device fully charged to school each day except Wednesday, sports day.
- b. Taking care of laptops in accordance with school guidelines.
- c. Adhering to [Online Communication Services: Acceptable Usage for School Students](#) policy.
- d. Backing up all data securely.

2. Acceptable computer and internet use

- a. Students are not to create, participate in, or circulate content that attempts to undermine, hack into and/or bypass the internet security mechanisms that are in place.
- b. Upon enrolment into a New South Wales Government school, parental/carer permission was sought to allow the student to access the Internet at school based on the *Online Communication Services: Acceptable Usage for School Students* policy. Extracts are provided below. This policy forms part of the Laptops User Charter. The [Online Communication Services: Acceptable Usage for School Students](#) policy (see below) applies to the use of the laptop and internet both on and off school grounds.

Extracts: [Online Communication Services: Acceptable Usage for School Students](#)

4.1 Access and Security

4.1.1 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 Communities.
- 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.

4.2 Privacy and Confidentiality

4.2.1 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.

4.3 Intellectual Property and Copyright

4.3.1 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.

4.4 Misuse and Breaches of Acceptable Usage

4.4.1 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.

5. Monitoring, evaluation and reporting requirements

5.1 Students will report:

5.1.1 any internet site accessed that is considered inappropriate.

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