



Bring Your Own Device (BYOD) Policy

Rationale

The aim of this policy is to ensure that all students in Years 3-6 of Wollongong West Public School have personal access to technology for educational purposes and to develop 21st Century learning skills in each student.

Bring your own device (BYOD) defines how staff, students and members of the school community can use their own devices to interact with the technologies used within the grounds of the school. This policy reflects the current practices of the wider community to have access to information when required.

The term “device” refers to any mobile electronic technology, including assistive technologies, brought into the school, which is owned by the student, and which has the capability of connecting to the department’s Wi-Fi network.

BYOD is an optional strategy.

Key reasons for implementing BYOD at Wollongong West Public School

- Devices are already a part of students’ lives

For a majority of our students, computers and portable devices such as phones and tablets are already integral to the world in which they live. We need to ensure that these devices are also a tool for learning (not just for play).

“By providing appropriate supervision and support we can help students develop cybersafety awareness and digital citizenship skills. By allowing students access to the same devices at school and at home, learning opportunities can extend to times and places outside of the classroom” (Horizon Project, 2013) and “allow students to work with technology with which they are already comfortable and familiar” (Horizon Project, 2013).

- Future focused learning

BYOD is about the meaningful integration of technology into students’ daily lives and developing the critical knowledge to use these tools effectively and appropriately. An environment where all

students have access to their own devices opens up new possibilities for collaborative and online learning, carefully structured and supervised by the teacher.

Students will be able to use their device as a means to communicate, calculate, photograph, video and edit across a range of different subjects.

Using the cloud

The NSW Department of Education has provided access for all students to Google Apps, an extensive suite of online software that allows students to collaborate online. This software provides new possibilities for our students including the ability to work together on a single document at the same time.

The cloud also has the advantage of being accessible from anywhere with Internet. This means that assignments from the classroom can be continued at home, seamlessly.

Equity

The implementation of a BYOD program can have significant effects on the overall access to devices for all students. We understand that not all students can afford to bring a device of their own to school.

At Wollongong West Public School we have invested substantial funds in the purchase of many laptops and mobile learning devices for student use. By encouraging students to bring their own device to school, this lessens the competition for school-owned devices and ensures greater access for everyone. Students without their own device will not miss out.

BYOD Implementation Actions and Responsibilities

Student and parent/carer responsibilities:

- Students may bring their own devices to school and may access the Department's Wi-Fi network.
- The device must meet the device specifications as outlined by the school.
- A device which does not meet the device specifications will not be permitted to access school networks and services
- The Department will provide Internet access at no cost to students enrolled in the school whilst at school.
- Students are responsible for the care and maintenance of their devices, including data protection and battery charging.

- Prior to bringing their device for the first time, students and their parent/caregiver must read and sign the BYOD Student Agreement which sets out the responsibilities and expectations relating to the use of personal devices.
- Students must follow teachers' directions as to the appropriate use of their devices in class.
- Insurance of a device is a responsibility of the parents/carers and can be covered via home and contents insurance. The school encourages parents to add a portability clause to their policy, so that the device is covered whilst outside the home.

Teacher responsibilities:

- Use of students' own devices in class is at the discretion of the teacher.
- Teachers will be responsible for supervising students in the safe use of devices online.
- Teachers will not be expected to provide technical support for students' devices or operating systems.

School responsibilities:

Wollongong West Public School will:

- Not accept any liability for the theft, damage or loss of any student's device. Students who bring their own devices onto school sites do so at their own risk.
- Not provide hardware or technical support for devices.
- Ensure all students have access to computing resources.
- Maintain a pool of devices for the use of students who do not have access to their own device.
- Provide a BYOD Student Agreement to list the responsibilities and expectations of each student.
- Ensure a copy of the BYOD Student Agreement is signed by each student and their parent/caregiver.
- Publish a device specification that outlines the requirements of the BYOD program devices, including but not limited to:
 - Form factor
 - Physical dimensions
 - Network connectivity
 - Operating system
 - Processor
 - Battery life

- Provide a wireless network with filtered Internet connection to which students may connect their personal device.
- Provide ongoing professional development for staff.

Whilst every measure will be taken to lock classrooms, we cannot guarantee a safe storage of devices throughout the day.

Inappropriate Use and Confiscation

Where the school has reasonable grounds to suspect that a device contains inappropriate data which breaches the BYOD Agreement, staff may:

- Temporarily confiscate the device for the purpose of confirming the existence of the material.
- Depending on the nature of the material involved, further action may be taken including referral to the police.
- School disciplinary action may also be appropriate, according to our Student Wellbeing Policy.

BYOD Device Requirements

Any device chosen by a student for school purposes must enable the student to complete the normal activities set as part of their education.

Please make sure your device meets our minimum specifications.

If you are unable to understand any other these features please talk to our staff.

Type of Device	<p>Students can bring a laptop or tablet to school. The laptop or tablet must meet the required specifications detailed below. Examples of suitable devices are iPads, Windows 8 or Android tablets, laptops and Chromebooks. Students may not use mobile phones for BYOD.</p> <p>Devices must be running the latest operating system version (Windows, Android, iOS, OSX, Linux and ChromeOS)</p>
-----------------------	--

Connectivity	Primary schools: The department's Wi-Fi network installed in primary schools operates on the 802.11n 5Ghz standard. Devices that do not support this standard will not be able to connect.
Memory and RAM	Tablets must have a minimum of 1GB RAM. Laptops require a minimum of 2GB RAM. Devices must have a minimum of 8GB storage.
External storage	Please ensure you back up your devices at home.
Battery Life	Minimum 3 hours Students must ensure they bring their device to school fully charged for the entire school day. No charging equipment will be supplied by the school.
Hardware features	Devices may have a built-in camera and built-in microphone.
Carry Case	Yes. Keep your devices safe using carry cases, screen guards, etc.
Insurance and warranty	Students and their parents/caregivers are responsible for arranging their own insurance and should be aware of the warranty conditions for the device.

BYOD Student Agreement

Prior to connecting their devices to the department's Wi-Fi network, students must return a BYOD Student Agreement.

The BYOD Student Agreement must be signed by both the student and by a parent/caregiver.

I agree that I will abide by Wollongong West Public School's BYOD policy and that:

- I will use the DoE's Wi-Fi network for learning.
- I will use my device during school activities at the direction of the teacher.
- I will not attach any school-owned equipment to my mobile device without the permission of the school.

- I will use my own portal/Internet log-in details and will never share them with others.
- I will stay safe by not giving my personal information to strangers.
- I will not hack or bypass any hardware and software security implemented by the department or my school.
- I will not use my own device to knowingly search for, link to, access or send anything that is:
 - offensive
 - pornographic
 - threatening
 - abusive or
 - defamatory
 - considered to be bullying.
- I will report inappropriate behaviour and inappropriate material to my teacher.
- I understand that my activity on the Internet is recorded and that 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 understand and have read the limitations of the manufacturer's warranty on my device, both in duration and in coverage.
- I have read the BYOD Student Responsibilities document and agree to comply with the requirements.
- I have reviewed the BYOD Device Requirements document and have ensured my device meets the minimum outlined specifications.
- I have read and will abide by the NSW Department of Education's Online Communication Services – Acceptable Usage for School Students.

Date: ___ / ___ / ___

Student name: _____ Signature: _____

In the presence of:

_____ Parent/caregiver _____ Parent/caregiver signature

Appendix 1:

Online Communication Services: Acceptable Usage for School Students

This document defines the policy for school students of the NSW Department of Education for the appropriate and acceptable use of internet and online communication services provided by the Department.

To access links visit the following:

https://detwww.det.nsw.edu.au/policies/general_man/general/accep_use/PD20020046_i.shtml?level=Schools&categories=Schools%7ccomputers+%26+internet%7conline+communication+services

1.Objectives - Policy statement

1.1

The internet provides an opportunity to enhance students' learning experiences by providing access to vast amounts of information across the globe. Online communication links students to provide a collaborative learning environment and is intended to assist with learning outcomes. Today's students are exposed to online communication tools and the internet in their community. They have the right to expect secure access to these services as part of their learning experiences with the NSW Department of Education.

1.2

Use of the internet and online communication services provided by the NSW Department of Education is intended for research and learning and communication between students and staff. Access to internet and online communication tools at school will assist students to develop the information and communication skills necessary to use the internet effectively and appropriately.

1.3

Responsible use of the services by students, with guidance from teaching staff, will provide a secure and safe learning environment.

1.4

Students using internet and online communication services have the responsibility to report inappropriate behaviour and material to their supervisors.

1.5

Students who use the internet and online communication services provided by the NSW Department of Education must abide by the Department's conditions of acceptable usage. They should be made aware of the acceptable usage policy each time they log on.

1.6

Students should be aware that a breach of this policy may result in disciplinary action in line with their school's discipline policy.

2.Audience and applicability

2.1

This policy applies to all school students located at NSW public schools who access internet and online communication services within the NSW Department of Education and Communities network and from any external location.

3.Context

3.1

This policy document takes account of the Memorandum *Student Access to the Internet* of 18 July 1997 and the Memorandum DN/04/00215 – *Review by Schools of their Student Access to the Internet Policies*.

3.2

This policy document should be read as consistent with school discipline, child protection, anti-discrimination and anti-racism policies.

3.3 Document history and details

4.Responsibilities and delegations

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:

- 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.

5.2

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.

6. Contact

Director, Learning Systems, (02) 9266 8951.