MITCHELL HIGH SCHOOL
Keyworth Drive Blacktown
mitchell-h.schools.nsw.gov.au
mitchell-h.school@det.nsw.edu.au
9622 9944

DEPARTMENT OF EDUCATION AND MITCHELL HIGH SCHOOL BRING YOUR OWN DEVICE (BYOD) STUDENT AGREEMENT

Students must read and sign the BYOD Student Agreement in the company of a parent or carer unless otherwise directed by the principal.

I agree that I will abide by the school's BYOD policy and that:

- ☐ I will use the department'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.

MITCHELL HIGH SCHOOL
Keyworth Drive Blacktown
mitchell-h.schools.nsw.gov.au
mitchell-h.school@det.nsw.edu.au
9622 9944

BRING YOUR OWN DEVICE (BYOD) STUDENT AGREEMENT

Students must read, tick the below box and sign the BYOD Student Agreement in the company of a parent or carer unless otherwise directed by the principal.

☐ *I have read and will abide by the NSW Department of Education Online Communication Services – Acceptable Usage for School Students.*

_____ _____

Student's Frist Name *Student's Surname*

_____ Date: _____/_____/_____

Student Signature

I have signed the BYOD Student Agreement form in the in the presence of:

_____ _____

Parent/Carer Name *Parent/Carer Signature*

Date: _____/_____/_____

BYOD DEVICE REQUIREMENTS

Wireless connectivity:

High schools: The department's Wi-Fi network installed in high schools operates on the **802.11n 5Ghz standard**. Devices that do not support this standard will not be able to connect.

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.

Note: There may be some variation to this standard in primary schools. The IT delegate in the school will be able to provide details.

***Operating system*:**

The current or prior version of any operating system.

Software and apps:

School-based requirements. All software and apps should be fully updated.

***Battery life*:**

A minimum of 5hrs battery life to last the school day.

***Memory and RAM*:**

A minimum specification of 16 GB storage and 2 GB RAM *to process and store data effectively.*

***Hardware features*:**

Camera and microphone.

Ergonomics:

Reasonable sized screen and a sturdy keyboard *to enable continuous use throughout the day.*

Other considerations

Casing: Tough and sturdy to avoid breakage.

Weight: Lightweight for ease of carrying.

Durability: Durable and strong.

Accessories

Carry case: Supply a carry case or skin to protect the device.

Insurance and warranty: Be aware of the terms of insurance policies/warranties for the device. The school will not accept responsibility for loss or breakage.

Back-up storage: Consider a portable hard drive as an appropriate source of back-up storage for essential documents.

BYOD STUDENT RESPONSIBILITIES

Operating system and anti-virus:
Students must ensure they have a legal and licensed version of a supported operating system and of software. If applicable, students' devices must be equipped with anti-virus software.

NSW Department of Education and Communities' Wi-Fi network connection only:
Student devices are only permitted to connect to the department's Wi-Fi network while at school. There is no cost for this service.

Battery life and charging:
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.*

Theft and damage:
Students are responsible for securing and protecting their devices at school. *Any loss or damage to a device is not the responsibility of the school or the Department.*

Confiscation:
Students' devices may be confiscated if the school has reasonable grounds to suspect that a device contains data which breaches the BYOD Student Agreement.

Maintenance and support:
Students are solely responsible for the maintenance and upkeep of their devices.

Ergonomics:
Students should ensure they are comfortable using their device during the school day particularly in relation to screen size, sturdy keyboard etc.

Data back-up:
Students are responsible for backing-up their own data and should ensure this is done regularly.

Insurance/warranty:
Students and their parents/caregivers are responsible for arranging their own insurance and should be aware of the warranty conditions for the device.

ONLINE COMMUNICATION SERVICES: ACCEPTABLE USAGE FOR SCHOOL STUDENTS

Outlines appropriate and acceptable student use of internet and online communication services provided by the department.

Bring Your Own Device (BYOD) is a program that permits students to bring their own electronic devices to school.

1. Objectives – DoE 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 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.

1.2 Use of the internet and online communication services provided by the department 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 department must abide by the 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 department 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.

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 department.
- 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.

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.