# MOOREBANK HIGH SCHOOL

# STUDENT BRING YOUR OWN DEVICE (BYOD) AND ACCESS TO THE INTERNET POLICY

Key principles

The Moorebank High School Bring Your Own Device (BYOD) Policy has been created in accordance to the DEC Student Bring Your Own Device Guidelines document. The BYOD Policy aims to provide an effective process that allows Moorebank High School to efficiently incorporate student-owned devices into our digital learning environment while maintaining the security of school and DEC infrastructure and data.

The device in BYOD refers to any of the following technologies:

* Laptops
* Netbooks
* Convertible laptop/windows compatible tablet

Access to the Digital Education Revolution (DER) network, will be made available to students who bring their own devices to school for appropriate learning activities in addition to accessing resources and research materials at no cost to the student.

1. Student BYOD Agreement
2. The Student BYOD Agreement is a document with the purpose of acknowledging acceptance and agreement of the terms associated with the school's implementation of the Student Bring Your Own Device (BYOD) Policy by both students and parents/carers. It is accompanied by an Information Sheet that must be provided in conjunction with the Student BYOD Agreement.
3. Prior to connecting their device to the network, students must return a Student BYOD Agreement. This agreement must be signed by the student and by a parent/carer. The principal may accept the student's signature for students living independently.
4. Students will be made aware of and agree to their obligations under the Student BYOD Policy prior to using their own device in Moorebank High School’s digital learning environment. School staff should endeavour to ensure that the BYOD student responsibilities are clearly understood by both students and their parents or carers.
5. By accepting the terms, the student and parents/carers acknowledge that they:

* Agree to comply with the conditions of the Student BYOD Policy.
* Understand that both the school and the DEC have the capacity to access their device and the data/information it contains at the Principal's discretion.
* Understand that under no circumstances will the DEC or the school accept any liability for the theft, damage or loss of any student's device.
* Understand that noncompliance may result in the withdrawal of BYOD permission and access.

1. The Student BYOD agreements needs to be retained in print or electronic form for future access as required.
2. Cost to Students
   1. Internet access through the Department's network will be provided at no cost to students in NSW Public Schools.
   2. Students will not be able to print from school printers using their BYO device. Access to school printers will be via the computers in the school Library. Students will require a USB storage device to transfer the files from their BYO device to the school computers.
3. Student and Parent/Carer Responsibilities

## **Students are solely responsible for the care and maintenance of their BYO devices.**

This includes but is not limited to:

1. Students are responsible for managing the battery life of their BYODs device and acknowledge that the school is not responsible for charging their devices. Students should ensure that their devices are fully charged before bringing them to school. Schools are not responsible for providing facility for students to charge their devices at school.
2. Student devices must meet the minimum device specifications including maintaining current antivirus software installed on their BYO device and must continue to maintain the latest service packs, updates and antivirus definitions.
3. Students should not attach any school-owned equipment to their BYO devices without the permission of the school principal or their delegate. This includes, but is not limited to, keyboards, mouses and connecting the BYOD device to the school network via a network cable.
4. Students should clearly label their BYOD device for identification purposes.
5. Students are responsible for securing and protecting their device in schools. This includes protective/carry cases and exercising common sense when storing the device. Schools are not required to provide designated or secure storage locations.
6. Students are responsible for ensuring the operating system and any software/data on their device is legally and appropriately licensed.
7. Students will use their BYOD device for educational purposes only during classes and will not connect to the internet using their own internet connection (if they have one), and therefore bypass DEC web filtering, whilst on the school grounds.
8. Students will bring their BYOD device everyday so that they are available for educational use in all classes.
9. Students without the financial capabilities for BYOD will be able to borrow an ex-DER laptop so that all students have access to online resources. The Principal or their delegate will determine the duration of the ex-DER laptop loan upon application from the student and their parent/ carer.
10. Damage and loss
11. Under no circumstances will Moorebank High School accept any liability for the theft, damage or loss of any student's device. Please refer to:
    1. <https://detwww.det.nsw.edu.au/media/downloads/directoratesaz/legalservices/ls/legalissuesbul/bulletin35.pdf>
    2. <https://detwww.det.nsw.edu.au/media/downloads/directoratesaz/legalservices/ls/legalissuesbul/bulletin8.pdf>
12. In cases of malicious damage or theft of another student's device, existing school processes for damage to school’s or another student's property apply.
13. Moorebank High School will regularly review policies and processes to include BYO devices where appropriate e.g. Student Welfare and Fair Discipline Code.
14. IT Support
15. Students will not receive ICT hardware or software technical support from the NSW DEC for their individual BYO device.
16. Moorebank High School Staff will only provide support and assistance with connecting the device to the school wireless system.
17. **Long-term care and support of BYO Devices**
18. Students and parents/carers are solely responsible for repair and maintenance of their own device. It is not the school's responsibility.
19. Warranties: Students and parents/carers should understand the limitations of the manufacturer's warranty on their BYO devices, both in duration and in coverage. Under Australian consumer legislation, warranties usually last for one year, during which any manufacturing defects will be repaired or the device will be replaced (as per the specific terms and conditions of the manufacturer).
20. Extended Warranties: At the time of purchase, students and parents/carers may also purchase an optional extended warranty (past the standard warranty period) from the supplier/manufacturer of their device, during which any manufacturing defects that may occur will also be repaired.
21. Insurance
22. Student BYO devices are not covered by Treasury Managed Fund.
23. Students may purchase an optional insurance policy from the supplier of their device or a relevant insurance company. As mobile devices are subject to a higher risk of accidental damage, prior to signing up for an insurance policy, parents/carers should be fully aware of the details and limitations of the policy, including any excess charged for making a claim, and the name of the company that holds the policy.
24. As a guide, a suitable BYOD device insurance policy should cover all types of BYOD devices and provide worldwide, replacement cost coverage against:
    1. accidental damage,
    2. damage from falls and liquids,
    3. theft
    4. fire
    5. vandalism
    6. natural disasters (such as floods, cyclones, earthquakes, tornados, water damage, and power surge due to lightning)
25. Acceptable use of BYO devices
26. Students must not use the Moorebank High School network services to seek out, access, store or send any material of an offensive, obscene, pornographic, threatening, abusive or defamatory nature. Such use may result in legal and/or disciplinary action, including suspension from school.
27. Students shall not create, transmit, retransmit or participate in the circulation of content on their devices that attempts to undermine, hack or bypass any hardware and software security mechanisms that have been implemented by the Department, its Information Technology Directorate DEC or MHS.
28. Students must not copy, transmit or retransmit any material that is protected by copyright, without prior permission from the copyright owner.
29. Students must not take photos or make video or audio recordings of any individual or group without the express written permission of each individual (including parent/carer consent for minors) being recorded and the permission of an appropriate staff member.
30. Students shall comply with departmental DEC or school policies concerning their use of BYO device at school and while connected to the Department's DEC network including:

* Online Communication Services- Acceptable Usage for School Students.
* Acceptable Use of Department's DEC portal services.

1. Students who use their devices inappropriately may have the device confiscated. Please refer to:

<https://detwww.det.nsw.edu.au/media/downloads/directoratesaz/legalservices/ls/legalissuesbul/bulletin56.pdf>

1. The principal retains the right to be the final arbiter of what is, and is not, appropriate use of BYO devices at Moorebank High School within the bounds of NSW privacy legislation.
2. The consequences of any breaches of this policy will be determined by the principal, in accordance with the school's Welfare and Discipline Policy.
3. Device Minimum specifications
4. Prior to purchasing or using an already purchased device, parents and students should be made aware of the following technology standards required for devices at MHS:
   1. Laptop; netbook or convertible laptop/tablet.
   2. Minimum screen size of 10 inches
   3. Minimum of 4GB RAM
   4. USB 2.0 (or better) Ports
   5. **Device MUST have 5 GHz wireless capability** (or the latest IEEE 802.11ac) in order to connect to the DEC wi-fi network
   6. Minimum battery life of 6 hours
   7. HTML5 web browser installed e.g.:
      1. Chrome 22 or later
      2. Internet Explorer 9 or later
      3. Safari 5.1.7 or later
      4. Firefox 16 or later
   8. Up to date antivirus installed
5. Other considerations when purchasing a device include:
   1. Extended warranty
   2. Device insurance
   3. Protective casing (scratch/impact/liquid-splash resistant)
   4. Additional or spare battery packs
   5. Ergonomics (is this device comfortable to use for an entire school day)
   6. Backup storage such as portable hard drive or USB flash drive
6. Security and device management processes
7. The network will become the point where DEC security policies are implemented.
8. There are a wide range of security considerations that will be addressed. These include but are not limited to:
   1. Strong passwords
   2. Device anti-virus software
   3. Data and network traffic encryption
   4. Privacy controls
   5. Internet filtering
   6. DEC antivirus
   7. DEC technology infrastructure security
   8. Student Cyber Safety
   9. Educational policies and security processes will be updated as required to ensure a secure and effective digital learning environment.
9. This policy should be read and interpreted in conjunction with:
   1. Code of Conduct Policy
   2. Copyright law of Australia
   3. Values in NSW Public Schools
   4. DEC Privacy Code of Practice
   5. Online Communication Services - Acceptable Usage for school students
   6. Legal Issues Bulletin No. 35 November 2012
   7. Legal Issues Bulletin No. 8 September 2012
   8. Legal Issues Bulletin No. 56 April 2015

**DEC Online Communication Services:**

**Acceptable Usage for School Students**

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

1. Objectives - Policy Statement

## 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 and Communities.

## Use of the internet and online communication services provided by the NSW Department of Education and Communities 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.

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

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

## Students who use the internet and online communication services provided by the NSW Department of Education and Communities 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.

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

1. Audience and Applicability

## 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.

1. Context

## 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.

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

1. 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 are 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 thee-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 e­learning 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.

1. 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.

1. Contact

Director, NSW Curriculum and Learning Innovation Centre, (02) 9715 8150