MHS BYOD Policy

MUDGEE HIGH SCHOOL STUDENT BRING YOUR OWN DEVICE (BYOD) POLICY

Introduction

This document provides advice and direction to students who choose to use BYOD to access the Department of Education (DOE) wireless network.

Key Principles

- The term "device" in this policy refers to any personal mobile electronic device with the capability to connect to the department's Wi-Fi network.
- Mudgee High School allows students to bring their own devices to school and provide access to the DOE's Wi-Fi network.
- The DOE will provide internet access through its wireless networks at no cost to students enrolled in NSW Public Schools at DOE sites.
- Students are responsible for the care and maintenance of their devices including data protection and battery charging.
- The department 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.
- Schools are not obliged to provide hardware or technical support for devices.
- Students and their parents/carers must complete and return a signed BYOD Agreement prior to connecting to the department's network.
- Where the school has reasonable grounds to suspect that a device contains data which breaches the BYOD Agreement, they may 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.

Student BYOD Agreement

- Prior to connecting their devices to the network, students must return a Student BYOD Agreement. This agreement must be signed by the student and by a parent/carer. If a student is living independently of their parents or is 18 years of age or more, there is no requirement to obtain the signature of a parent.
- It is important to ensure that students are aware of and agree to their obligations under the Student Bring Your Own Device (BYOD) Policy and relevant policies, prior to using their own device on the DOE Wi-Fi network. School staff should endeavour to ensure that the BYOD student responsibilities are clearly understood by both students and their parents or carers.
- The Student BYOD Agreement is a simple 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 provided in conjunction with the Student BYOD Agreement. 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 noncompliance may result in the student being subject to school disciplinary action.

Cost to Students

Internet access through the Department's network will be provided at no cost to students enrolled in NSW Public Schools at DOE sites.

Student Responsibilities

- Students are solely responsible for the care and maintenance of their BYO devices. This includes but is not limited to:
  - Managing battery life and regular charging of their device.
  - Labelling their device for identification purposes.
  - Purchasing and using device protective casing.
  - Ensuring the device is safe and secure during travel to and from school and throughout the school day.
  - Maintaining up-to-date anti-virus software and operating system on their device.
  - Taking insurance coverage of their own device to protect any accidental damage, theft or loss.

1. Students are responsible for managing the battery life of their 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 (or restricted from) providing facilities for students to charge their devices.
2. Students must have a supported operating system and current antivirus software installed on their 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 mobile devices without the permission of the school principal or their delegate.
4. Students should clearly label their BYOD device for identification purposes. Labels should not be easily removable.
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 all software on their device is legally and appropriately licensed.

Damage and loss

Students bring their devices onto the school site at their own risk. For advice on theft or damage of students' personal devices refer to legal issue bulletins below:

- https://detwww.det.nsw.edu.au/media/downloads/directoratesaz/legalservices/ls/legalissuesbul/bulletin35.pdf

- https://detwww.det.nsw.edu.au/media/downloads/directoratesaz/legalservices/ls/legalissuesbul/bulletin8.pdf

  In cases of malicious damage or theft of another student's device, existing school processes for damage to schools or another student's property apply.

Technical Support

- NSW DOE staff are under no obligation to provide any technical support on either hardware or software.

Long-term care and support of BYODs

- Students are solely responsible for repair and maintenance of their own device. It is not the school's responsibility.
- Warranties: Students 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).
- Extended Warranties: At the time of purchase, students 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.

Insurance

- Student BYO devices are not covered by Treasury Managed Fund. When students purchase their BYO device, they may also 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, students 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. As a guide, a suitable BYOD device insurance policy should cover all types of BYOD devices and provide worldwide, replacement cost coverage against:
    - Accidental damage
    - Damage from falls and liquids
    - Theft
    - Fire
    - Vandalism
    - Natural disasters (such as floods, cyclones, earthquakes, tornados, water damage, and power surge due to lightning

Acceptable use of BYO devices

- Using the DOE network services to seek out, access, store or send any material of an offensive, obscene, pornographic, threatening, abusive or defamatory nature is prohibited. Such use may result in legal and/or disciplinary action.
- 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 or the school.

- Students must not copy, transmit or retransmit any material that is protected by copyright, without prior permission from the copyright owner.
- Mobile phone voice and text, SMS messaging or device instant messaging use by students during the school hours is a school based decision.
- 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.
- Students shall comply with departmental or school policies concerning the use of BYODs at school and while connected to the Department's network including:

  Online Communication Services – Acceptable Usage for School Students
- The principal retains the right to determine what is, and is not, appropriate use of BYODs at the school within the bounds of NSW privacy and other legislation.
- The consequences of any breaches of this policy will be determined by the Principal, in accordance with the school's welfare and discipline policies. As the student device is intended as a personal learning tool schools are encouraged to consider a variety of alternatives to ensure equitable access to continued learning opportunities.

DOE Technology Standards

Prior to purchasing or using an already purchased device, parents and students should be made aware of the following technology standards required for devices used within schools:

- The DOE wireless network installed in high schools only operates on the 802.11n 5Ghz standard. Devices with 802.11a/b/g or 802.11n 2.4Ghz only may not be able to connect.
- The battery life of the device should be capable of lasting 6 hours minimum of constant use without charge
- Device hardware specifications must meet the minimum (ideally the recommended) specifications of the operating system and all applications
- Currently supported Operating System

Other considerations when purchasing a device include:

- Extended warranty
- Device insurance
- Protective casing (scratch/impact/liquid-splash resistant)
- Additional or spare battery packs
- Ergonomics (is this device comfortable to use for an entire school day)
- Backup storage such as portable hard drive or USB flash drive

Security and device management processes

Students using BYOD at Mudgee High School should consider the following aspects of safe computer use.

- Strong passwords
- Device anti-virus software
- Data and network traffic encryption
- Privacy controls
- Internet filtering
- DEC technology infrastructure security
- Student Cyber Safety

NB. The act of accessing the MHS computer network implies that the user is aware of and agrees to abide by the code of behaviour statements contained in the DOE communications policy and the MHS BYOD Student Agreement.

*** This BYOD Policy is subject to review and updating in accordance with changes to the school's technology requirements.**