ELECTRONIC DEVICES AND INTERNET USAGE CHARTER

1. Purpose
Muirfield High School’s Bring Your Own Device (BYOD) Program gives freedom to students and their families to tailor their choice of technology to their own educational needs and personal preferences. Muirfield High School will facilitate this in accordance with the BYOD Policy. However, students and parents must be aware of and consent to the program’s boundaries described in the Electronic Devices and Internet Usage Agreement.

This charter incorporates the use of mobile phones. Many students possess smart phones which they use in place of tablets or computers. It is also accepted that many parents wish their children to have mobile phones in their possession during the school day. For this reason there is no ban on mobile phone possession at school.

The Charter also applies to students during school excursions, camps and extra-curricular activities.

2. Scope and Definitions
2.1 Parties
This agreement is between Muirfield High School, a student currently attending or who will be attending Muirfield High School and their parent or carer.

2.2 “Student” and “Students”
Reference in this agreement to student or students means a student currently attending or who will be attending Muirfield High School and binds his/her parent or carer.

2.3 “Bring Your Own Device User Charter”
This agreement may be referred to as the Bring Your Own Device (BYOD) User Charter or Electronic Devices and Internet Usage Charter.

2.4 “Device”
Reference in this agreement to device means any electronic device brought by a student to Muirfield High School. The term device refers to any personal mobile electronic device which can connect to the Department’s Wi-Fi network or to the Internet via 3G or 4G and can store information. It also includes storage devices, such as USBs and media devices, such as iPods.

3 Equipment
3.1 Custodianship
The device brought to school pursuant to this policy is to be solely the student’s to use throughout the school day.

3.2 Choice of equipment
Families have a wide choice of device as most devices connect to Muirfield’s Wi-Fi network. If families are unsure whether their device will connect, they can speak with the TSO.

3.3 Damage or loss of equipment
3.3.1 Students bring their own device for use at Muirfield High School at their own risk.

3.3.2 Muirfield High School will not be responsible for any loss, theft or damage to:
(a) the device
(b) data stored on the device while the device is at school or during a school-related activity.

3.3.3 Parents and students should consider whether their device requires insurance and whether specific accidental loss and breakage insurance is appropriate for the device.
3.3.4 In circumstances of malicious damage or theft of a student’s device, existing school processes for the damage to school or another student’s property apply. The Principal will, having regard to all the circumstances of the matter, determine whether the other student is responsible for the damage to the device and whether costs incurred in the repair of the device should be borne by the other student.

3.3.5 In accordance with clause (6.4) below, students should not bring peripheral equipment, including power charges and cables to school with their device. Liability for damage or loss of peripheral equipment will in all circumstances be borne by the student.

4. Standards for equipment care
4.4.1 Students are responsible for:
(a) taking due care of their device.
(b) adhering to the Department of Education and Communities’ policy Online Communication Services: Acceptable Usage for School Students (PD/2002/0046/V04).
(c) backing up all data securely. All electronic data and resources used for school coursework must be stored on another device or electronic medium accessible on demand. Students must not rely on the continued integrity of data on their device.
(d) ensuring the operating system and all software on their device are legally obtained and appropriately licenced.

4.2 Students should clearly label their device for identification purposes.

5. Misuse of equipment and communication systems
5.1 Standard school discipline procedures apply for misuse of the device as outlined in this Charter or other school rules.

5.2 The consequences of any breach will be determined by the Principal, in accordance with the school’s discipline code and welfare practices. Examples of action the school may take in cases of misuse include:
(a) the teacher will direct the student to pack away the device for the remainder of the lesson
(b) the device is taken away by a Head Teacher or Deputy Principal for the remainder of the school day and/or until a parent or carer picks up the device
(c) permission for the student to bring their device to school pursuant to the Bring Your Own Device policy is revoked
(d) student access to the Department’s Wi-Fi network is disabled
(e) conventional discipline procedures, including detention or suspension where deemed appropriate, pursuant to the school’s discipline procedures.

6. Acceptable equipment and communication system use
6.1 Use of the device during the school day is at the discretion of teachers and staff. Students must use their device as directed by their teacher. Devices should not be used in any manner or place that is disruptive to learning or the normal routine of the school.

6.2 The primary purpose of the device at school is educational. Mobile voice, text, SMS or device messaging should be off or on silent at school. The learning environment should not be disrupted by ringtones, music or other sounds or non-educational uses of the devices. Phone calls must not be made or answered during class time.

6.3 Students’ own device is to be charged at home. The school does not provide charging facilities or connectivity cables.
6.4 Students should avoid bringing peripheral device equipment to school with the device. Peripheral equipment includes:
   (a) chargers
   (b) charging cables
   (c) docking cradles, with the exception of a docking cradle that includes a keyboard integrated into the peripheral
   (d) adapters for the connection of video output or data transfer

6.5 While at school, all material on the device, including peripheral storage devices, is subject to review by school staff.

6.6 Students are to connect their device to the designated wireless network only. Students are not to utilise the school’s wired network to connect their device.

6.7 Students are not to create, participate in, or circulate content that attempts to undermine, hack into and/or bypass the hardware and software security mechanisms that are in place.

6.8 Students must not take photos or video or audio recordings of any individual or group without the express written permission of each individual (including parent/career consent for minors) being recorded and the permission of an appropriate staff member.

6.9 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 Department of Education and Communities' policy Online Communication Services: Acceptable Usage for School Students (PD/2002/0046/V04). Extracts are provided below. This policy forms part of this Bring Your Own Device User Charter.

6.9 The policy Online Communication Services: Acceptable Usage for School Students (PD/2002/0046/V04) applies to the use of the device and internet on the device:
   a. at school
   b. to access school-hosted systems
   c. in connection with a school-related activity or school-related program, including coursework.

6.10 The Principal retains the right to determine what is, and is not, appropriate use of devices at school within the bounds of NSW privacy and other legislation and Departmental policy.

7. Equity
7.1 All students, no matter their families’ financial means, have access to computing resources in the school.
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:
  1) a message that was sent to them in confidence.
  2) computer virus or attachment that is capable of damaging recipients’ computers.
  3) chain letters and hoax emails.
  4) spam, e.g. unsolicited advertising material.
• never send or publish:
  1) unacceptable or unlawful material or remarks, including offensive, abusive or discriminatory comments.
  2) threatening, bullying or harassing another person or making excessive or unreasonable demands upon another person.
  3) sexually explicit or sexually suggestive material or correspondence.
  4) 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.