

## MANDATORY BRING-YOUR-OWN-DEVICE (BYOD) ACCEPTABLE USE POLICY

### Preamble

At Mount Annan Christian College, we recognise that the use of technology in our society has grown tremendously and for most young people it is a vital connection to the world around them. Personal devices can enhance and enrich learning opportunities both at home and at school. While we believe there is no substitute for sound teaching and learning practices, we also recognise the potential value of technology in shaping our students' educational experiences and the new avenues it can offer for learning.

### 1. Purpose

1.1 As we prepare students for life in the 21<sup>st</sup> century we must equip them with the skills to utilise technology responsibly and empower them for lifelong learning. To do this effectively, we are introducing a mandatory 'Bring Your Own Device' (BYOD) policy for students in Years 5 to 12.

This policy is about more than just enabling students to have a device and connection to the College wireless network. We believe that placing the technology of choice into the hands of our students

- provides opportunity for individualised learning,
- increases independence, creativity, innovation and
- promotes self-initiated learning within and beyond the classroom.

1.2 This policy allows students to use the device with which they are most comfortable and with which learning will be most effective. Recognising the importance of choice, we are not recommending specific brands and models of devices. Instead, we are specifying the minimum requirements to which each device should conform.

1.3 Students, their parents or guardians must read, understand and abide the BYOD Acceptable Use Policy before students are given permission to connect to the College wireless network.

1.4 The BYOD Acceptable Use Policy also applies to students during school excursions, camps and extra-curricular activities or the like.

### 2. Rationale

2.1 Personal devices have the capacity to enhance student productivity, extend the range of learning opportunities, such as through Project-Based Learning, and broaden engagement with the digital world when used in the proper context. They can provide a gateway to innovative ways of engaging with course content, increase intellectual stimulation and build confidence. They can also help accommodate individual learning styles and increase autonomy if used appropriately in the school environment.

2.2 The availability and appropriate use of these resources provide opportunities that can help students develop spiritually, academically, socially and physically. However, their inappropriate use can be detrimental to the teaching / learning process, be anti-social, and even harmful.

### **3. Responsibility**

3.1 It is the responsibility of students who bring devices to school to abide by the guidelines outlined in this document. Students accept the responsibility for the use of devices at school.

3.2 It is a matter for the College to indicate to students which devices may or may not be used at specific times and places, and in which ways they may or may not be used. Students should not presume the right to use a particular device in any circumstance.

3.3 Year 11 and Year 12 students, and other students who are undertaking non-face-to-face or independent learning sessions, may use a device for educational purposes and to facilitate study, and must ensure that they are not distracting other students.

3.4 When permission for use is granted within a classroom or during other school activity, it should be understood that use is limited to that particular classroom or event. The use of devices will be subject to teacher discretion at all times.

3.5 Students are responsible for the security of their own devices. Devices may be secured within the lockers provided by the College and it is up to each student to ensure this occurs. Students in Years 5 and 6 will have a dedicated space within their classroom for safe keeping of their device during the school day.

3.6 The College takes no responsibility for damage or theft of a student's device.

3.7 Students and/or parents must ensure the maintenance or upkeep of any personal device (ensuring anti-virus software is installed and upgraded, keeping it charged, installing updates or upgrades, fixing any software or hardware issues). School licenced software will not be installed on student personal devices.

3.8 Students must bring their device to school fully charged as limited opportunities will be available to charge their device at school.

### **4. Acceptable Uses**

4.1 The use of a personal laptop during the school day is at the discretion of teachers and staff. Students must use these devices as directed by their teacher.

4.2 The primary purpose of the use of personal devices at school is educational.

4.3 The use of a personal device is not to be a distraction in any way to teachers or students. The use of personal devices must not disrupt class in any way.

4.4 Students are permitted to use personal devices appropriately and responsibly outside scheduled classroom times (i.e. recess or lunch).

4.5 Students agree not to attempt to circumvent the school's network security and/or filtering policies. This includes setting up proxies and downloading programs to bypass security.

4.6 In using their devices students are expected to comply with the standards and act within the ethical framework of this College, where respect for individuals, their good name and dignity is paramount.

4.7 In some situations, such as formal Examinations, other specific rules may apply to devices. These will be outlined clearly and must be adhered to fully.

## **5. Unacceptable Uses**

5.1 A staff member who has reasonable grounds to suspect that a device may be being used inappropriately or has been used inappropriately may inspect any device brought onto the College campus by a student and refer the incident to the Head of School.

5.2 Accessing the wireless network other than through the College network is strongly discouraged. All devices brought to College should use the College wireless network. Students are not to deliberately access inappropriate material, such as websites, games, videos, music etc. If this should happen by accident, the following procedure MUST be followed immediately:

- i. Minimise the site immediately – without communicating to other students.
- ii. Inform the nearest teacher. (The site will then be blocked).

5.3 Students must not post photographs, personal information or refer in any way to members of the Mount Annan Christian College community (staff, students and parents – past and present) on the Internet without the permission of the School. This includes personal 'blogs', social media and networking sites as well as websites. Students must not refer to the school in any way, nor post images of themselves or others in school uniform on the Internet unless on a school sanctioned website or with the permission of the School.

5.4 Using devices to bully and threaten other students is unacceptable and will not be tolerated. In some cases it can constitute criminal behaviour. Devices and the use of the wireless network must not be used to harass, sexually harass or victimise other students or staff. Devices must not be used to violate a person's right to privacy or to view or transmit sexually explicit material.

5.5 It is forbidden for students to "gang up" on another student and use their devices to take videos and pictures of acts to denigrate and humiliate that student and then send the pictures to other students or upload it to a website for public viewing. This also includes using devices to photograph or film any student or staff member without their consent.

5.6 Devices are not to be used or taken into change rooms or toilets or used in any situation that may cause embarrassment or discomfort to their fellow students, staff or visitors to the school.

5.7 Should there be repeated disruptions to lessons caused by devices; the responsible student may face disciplinary actions as sanctioned by the Head of School.

5.8 Students should use devices for positive purposes: for learning, for legitimate communication, and for relaxation in acceptable ways. Devices must not be used to harass or victimise other students or staff, or to abuse a person's right to privacy (for example, taking, storing and then using a digital photo/video without a person's permission).

5.9 Students must not use the wireless network to download content such as music, videos, large movies, software, games, updates etc. for personal and non-educational use without the permission of the College.

## **6. Theft or damage**

6.1 Students should mark their devices clearly with their names.

6.2 Students who bring devices to school should leave them locked away in their locker/bag when they arrive. To reduce the risk of theft during school hours, students who carry devices are advised to keep them well concealed and not 'advertise' they have them.

6.3 Devices that are found in the school and whose owner cannot be located should be handed to Student Services.

6.4 The school accepts **no responsibility** for replacing lost, stolen or damaged devices.

6.5 The school accepts **no responsibility** for students who lose or have their devices stolen or damaged while travelling to and from school.

6.6 It is strongly advised that students use passwords to ensure that unauthorised access cannot be made on their devices (e.g. by other students, or if stolen). Students must keep their password confidential. Passwords may not be shared.

## 7. Consequences for Misuse/Disruption

7.1 One or more may apply;

- 7.1.1 The device is taken away for the Learning Session or the rest of the school day.
- 7.1.2 The device is taken away and kept within Student Services until a parent/guardian picks it up.
- 7.1.3 The student is refused permission to use personal devices at school.
- 7.1.4 Disciplinary action including detention, suspension or expulsion may be imposed.

7.2 Should the device be used to capture content at school that is inappropriate or harmful to another student (or teacher) and that student then chooses to post this content on the Internet or in any other public arena, the student will be subject to the same discipline as if they had been found with this content on the school premises.

7.3 As set out in the previous section, failure to heed the rules set out in this policy document may result in an alleged incident being referred to the police for investigation. In such cases, the parent or guardian would be notified immediately.

### General Information

Access to the Mount Annan Christian College wireless network, whether with school-provided or personal devices, is filtered in compliance with the College Mandatory BYOD Acceptable Use Policy. However, access from personal devices is limited to Internet and email use only. Students will not have direct access to any documents that reside on the school network from their personal devices.

**Access to the Mount Annan Christian College wireless guest network is a privilege, not a right.** Any use of the wireless network entails personal responsibility and compliance with all school rules and the College BYOD Acceptable Use Policy. In using the College network you willingly grant IT staff permission to conduct any necessary investigations regarding inappropriate Internet use at any time.

### Broadly, what device is suitable and what is not suitable?

Preferably, all students must have a laptop device with a dedicated keyboard (not just an 'on-screen' keyboard) running Windows 10, or any Apple Mac laptop. Devices that are dual laptop/tablet hybrids such as the Microsoft Surface are acceptable, so long as they have a dedicated keyboard and trackpad (which is often built into the case).

We do not recommend any device running Windows RT, any devices described as Google Chromebooks or running the Android operating system, nor do we recommend iPads/tablets.

Any device below a certain physical size would be impractical. Some micro-sized PCs with tiny screens and tiny keyboards will not be suitable. We suggest a 10.5 inch screen as a minimum.

We do not require devices that have their own separate 'cellular' internet connection.

In the first instance, the College minimum requirements to which each device should conform include:

**M:** Minimum **R:** Recommended

Laptop	Windows	Mac
Storage	<b>M:</b> 256GB Solid State Drive (SSD)	<b>M:</b> 256 GB Solid State Drive (SSD)
Memory (RAM)	<b>M:</b> 8GB	<b>M:</b> 8GB
Operating System	<b>M:</b> Windows 10	<b>M:</b> Yosemite 10.10 R: El Capitan 10.11
CPU	<b>M:</b> Intel R Core I5 or AMD Ryzen 5 or better	<b>M:</b> Intel R Core I5
Wi-Fi	<b>M:</b> 802.11b/g/n	<b>M:</b> 802.11b/g/n
Battery Life	<b>M:</b> 6 Hours <b>R:</b> 8 Hours	<b>M:</b> 6 Hours <b>R:</b> 8 Hours
Screen Size	<b>M:</b> 10.5 inches	<b>M:</b> 10.5 inches
Required Accessories	Protective sleeve, bag or satchel Headphones	Protective sleeve, bag or satchel Headphones

What you need to be able to do:	What you need installed ready to go:	Related Links
<b>Create and edit the following:</b>		
- Documents - Spreadsheets - Presentations	Microsoft Office 2013+ (Word, Excel, PowerPoint) or iWork (Pages, Numbers, Keynote) or Open Office 4.1.2 (Win & Mac)	<a href="http://openoffice.org">openoffice.org</a>
- Audio Files	Audacity 2.1.1 (Win & Mac) or Garage Band (Mac)	<a href="http://audacity.sourceforge.net">audacity.sourceforge.net</a>
- Video Files	Edit - <b>M:</b> Windows Movie Maker or iMovie View - <b>R:</b> VLC Media Player	<a href="http://videolan.org">videolan.org</a>
Submit documents in common formats	iWork and Open Office have the inbuilt ability to export to Microsoft Office and PDF formats	
Up-to-date Anti-Virus	Bitdefender or Forticlient for Windows systems	<a href="http://bitdefender.com.au">bitdefender.com.au</a> <a href="http://forticlient.com/downloads">forticlient.com/downloads</a> ( Please note you will have to scroll down the website to find the download for Forticlient)
Browse the Internet	Latest version of Chrome or Internet Explorer / Safari	<a href="http://google.com/chrome">google.com/chrome</a> <a href="http://mozilla.org/en-GB/firefox">mozilla.org/en-GB/firefox</a>
Up-to-date Flash Player	Adobe Flash Player	<a href="http://get.adobe.com/flashplayer">get.adobe.com/flashplayer</a>
View PDF Files	Adobe Reader DC (Win & Mac)	<a href="http://get.adobe.com/reader">get.adobe.com/reader</a>

### Care and maintenance

Personal computers should be kept in a protective sleeve, bag or satchel, and we will require adequate protection be purchased for your device. The device and the sleeve/bag should have the students name on it.

### Backup of Data / Information

One important skill '21st Century Learners' need to cultivate is to backup data against accidental loss. Students should back up their important data to external USB devices like large capacity thumb drives or external hard disk drives. They may also make use of cloud based storage such as Dropbox or Google Drive. Students are responsible for safeguarding their data.

### **What if my child's laptop is out of action for any reason?**

Your child's teachers need to be told if their laptop is out of action for any reason, and it is your responsibility to make every effort to minimise the downtime. The school has limited capacity to loan any student a laptop, and even then it will be limited to use on school premises.

### **Student Electronic Mail (email) @student.macc.nsw.edu.au**

- All student Electronic Mail (email) @student.macc.nsw.edu.au accounts are property of Mount Annan Christian College. The College, at its discretion, may close the accounts at any time it deems necessary.
- The primary purpose of the MACC student email is educational. That is, the accounts are provided for students to communicate effectively internally and externally of the College, to be able to obtain external resources related to schoolwork, and to enable students to collaborate on school activities using google classroom.
- Messages that are sent or received by College email are not confidential. Although the College does not make a practice of monitoring electronic mail, the College reserves the right to retrieve the contents of user mailboxes for legitimate reasons, such as to find lost messages, to conduct internal investigations, to comply with investigations of wrongful acts, or to recover from system failure.
- Account usernames and passwords will be provided to parents upon request, so that parents can monitor the account if they wish.
- Communication through the College email system will exhibit common sense and politeness.
- Students are responsible for messages sent from their accounts.
- Students should not share their passwords.
- Messages posted on the College email system are not to cause disruption to the school environment or normal and acceptable school operations. Occasional and reasonable personal use of the College email is permitted, provided that this does not interfere with the performance of the email system or disrupt the operation of the College.
- Students must not identify their telephone numbers or home addresses in any email correspondence.
- Students will report to the Head of Secondary any unusual or suspicious email activities such as "spam" communications, obscene email including images, offensive or suspicious communications, or attempts by adults to lure them into dangerous behaviours, etc.
- System administrators may create filters to scan for and eliminate viruses and/or large files that are unrelated to the school operation.
- Use of the College email system is a privilege. Its use will align with the College rules and Student Management System and it will be used for discipline purposes if needed. Improper use of the system will result in disciplinary consequences that may include having access to emails temporarily or permanently revoked.
- When issues of concern arise, the College will deal directly with the student and/or parents/guardians. Illegal activities on the system will be referred to law enforcement authorities for appropriate legal action.
- Student email accounts will be removed from the system after graduation or leaving the school.

**Updated:** 29/10/2021