



BYOD (Bring Your Own Device) and IT USE CHARTER

1. The Purpose

The Mandurah Baptist College BYOD (Bring Your Own Device) Program aims to improve student learning experiences both in and out of the classroom. Families purchase a personal device for their student/s on the expectation that they will make good decisions regarding their personal use of technology. The College reserves the right to make decisions relating to access to the College network and students' use of devices on site.

2. Equipment

2.1. Ownership

- Parents/guardians purchase the BYOD device and have sole ownership of the device.
- Students must bring the device fully charged to school every day.
- All material on student devices is subject to review by school staff if deemed necessary.
- If there is a police request, Mandurah Baptist College will provide access to the device and network records associated with the use of the device.
- BYOD devices require the installation of the Microsoft Intune Company Portal software/app in order to access the College network. Installation of this app manages the device's connection to the College's network and resources, but should not interfere with the device's operation outside of the College (e.g. at home).

2.2. Damage or loss of equipment

- Devices that are damaged or lost by neglect, abuse or malicious act, will be the responsibility of the parents/guardians.
- It is recommended that parents/guardians purchase an extended manufacturer's warranty.
- In the case of suspected theft, the College should be informed immediately. Families may also elect to make a police report; in this case the event number should be provided to the College.
- Parents/guardians will be required to replace lost or damaged devices as soon as possible.
- It is recommended that parents/guardians/students have BYO devices on their "find my" app via iCloud (only available for Apple devices), in order to enable additional protection via "lost mode" in the event that the device is lost or stolen.

3. Standards For Device Care

The student is responsible for:

- Taking care of the device.
- Adhering to the acceptable usage requirements set out in this policy.
- Backing up all data securely.

4. Acceptable Device and Internet Use

*Please note that the provisions of this section apply to BYOD program devices **and** to College devices that students may use during the course of their educational program (e.g. desktop computers etc.).*

- 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 (e.g. VPNs, hot-spotting).
- Students are not to photograph or film other students or staff members without permission.
- Students are not to use their devices in any way that contravenes state or federal laws.
- Never knowingly initiate or forward e-mails 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 e-mails.
 - Spam, e.g. unsolicited advertising material.
- Students are not to send or publish:
 - Unacceptable or unlawful material or remarks, including offensive, abusive or discriminatory comments.
 - Threatening, bullying or harassing material to another person or make excessive or unreasonable demands upon another person.
 - Sexually explicit or sexually suggestive material or correspondence.
 - False or defamatory information about a person or organisation.
- Students must 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.
- Students should be aware that all use of the internet and online communication services can be audited and traced to the student accounts of specific users
- Students should not interfere with, or touch without permission, another individual's device, or devices belonging to the College
- All inappropriate use of devices will be subject to the College's Discipline Policy.

5. Access and Security

- Students will 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 student account.
- Promptly tell their supervising teacher if they suspect they have received a computer virus or spam (i.e. unsolicited e-mail) or if they receive a message that is inappropriate or makes them feel uncomfortable, including requests for excessive personal information or in-person meetings,

6. Privacy and Confidentiality

Students will:

- Never publish or disclose the e-mail 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.

7. 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 student 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.

8. Monitoring, evaluation and reporting requirements

Students will be aware that:

- Their usage of College networks and resources will be monitored (e.g. through the College's firewall)

Students will report:

- Any internet site accessed that is considered inappropriate.
- Any suspected technical security breach involving users from other schools, or educational institutions.

9. Alternative Devices

Please note that the provisions of this charter will apply to any device brought onto the premises by a student for educational purposes to the College and connected to the College network.