

Timbarra P-9 College – BYOD

Device Management

Prior to a BYO device being enrolled into the BYOD program, parents/carers are required to provide consent through Compass for the device to be managed by the College. The scope of management will be purely dedicated to the purpose of configuring BYO devices for school use.

Examples of management include, but are not limited to:

- Automatic installations for critical learning applications
- Configuration of access to school resources
- Automatic file backup using OneDrive
- Restrictions to prevent installation of unauthorized applications
- Enhanced security features (Antivirus protection, device hardening, file encryption)

In addition to the above, students will use a managed web browser with restricted settings which will prevent private browsing or deleting browsing history. Student accounts and browsing history may be accessed by the College under the context of an investigation in the event that the College is made aware of a breach of acceptable use of devices.

Due to the restrictions applied, students will be unable to install unauthorised applications on their device. During the time the device is managed by the College, the need for non-school use programs may arise. The College may allow installations of such programs where there is a justifiable use case and there is no impact on the College's management of the device. To request software installations, please email the College with the subject line **Software Request - <STUDENT NAME>** and details of the use case for the application.

Although the device itself will have restrictions applied, the College is unable to enforce restrictions on web browsing when the device is not connected to the College's Wi-Fi. We ask that parents utilise parental controls on their home router to manage web filtering restrictions at home. The College will not accommodate requests for the installation of monitoring/filtering software on the device itself, as these programs can often interfere with the College's ability to manage the device.

Over time, the College may make changes or adjustments to the configuration of devices as necessary to improve the security and safety of students.

During the device enrolment process, all existing data and user accounts on the device will be deleted. The College does not take responsibility for the recovery of existing data.

Following the device enrolment process, the student will only be able to access the device using their school-provided login details. Personal accounts will not be able to be added to the device, but the student will be able to use their device at home using their school account.