CHARLTON BROWN.

<div style="text-align:center">

POLICY

</div>

Policy Name:	**Information Technology and BYOD Policy**
Document Number:	IT 8.1.01
Approved by:	CEO
Last Approval Date:	May 2022
Review Date:	May 2022
Audience:	Charlton Brown Staff, Students and Community
Contact Officer:	IT Manager
Related Documents:	Privacy Policy; Student code of Conduct;
Legislation:	Education Services for Overseas Students Act 2000
	National Vocational Education & Training Regulator Act 2011
	Education (Accreditation of Non-State Schools) Act 2017
	National Code of Practice for Registration Authorities & Providers of Education and Training to Overseas Students 2018
	Standards for Registered Training Organisations 2015
	Education (Accreditation of Non-State Schools) Regulation 2017

1. Purpose

This policy lays out the Charlton Brown College approaches to facilitate good digital citizenship amongst its student body. The policy also outlines the Bring your Own Device (BYOD) program, including providing families with devices specification and other technology requirements.

This policy outlines the guidelines for student s use of Charlton brown networks, systems and devices, to allow students to take ownership of and responsibility for their technology.

2. Scope

This policy document is applicable to all students of Charlton Brown College. The policy is therefore applicable to parent/guardians of Charlton Brown College students

3. Policy Statement

Technology has become inextricable from our lives, and our relationship to it and each other is changing. Much contemporary curriculum focuses on how to ride these changes; our philosophy applies a more proactive approach. Young people will ultimately define the forms and functions of emerging digital communities. Charlton Brown College provides an environment in which young people develop the attributes to build these communities in a way that is healthy and for everyone.

At CHARLTON BROWN College one of our goals is the building of holistic attributes both on and off campus, and this policy aims to encompass the use of all technology (personal computers, school technology, mobile phones, cameras, social media etc.). Charlton Brown College adopts a forward-thinking approach which includes cloud-based content creation and collaboration, a contemporary learning resource centre, and, where practicable, paperless distribution of information.

Charlton Brown utilises a *Bring Your Own Device* (BYOD) program, acknowledging students will develop their own digital workflows and practices. Charlton Brown College similarly recognises that there are occasions when it is genuinely appropriate and beneficial for students to have access to mobile phones during the school day.

4. Digital Citizenship Practices

Charlton Brown College supports the development of the following digital citizenship practices, helping young people build healthy and productive digital communities. We teach these values through modelled behaviour, discussion, and engagement of the community.

Knowledge:
➢ Know the risk associated with the content you publish online.
➢ Protect your data with strong password practices.
➢ Spot and report scams where possible.
➢ Determine credible information.

Caring:
➢ Us the power of technology to spread kindness, not hate.
➢ Offer technological support to others if you have the skills.
➢ Encourage your friends to speak up against cyberbullying.
➢ Support victims of cyberbullying.

Communicators:
➢ Treat online communication as face-to-face
➢ Block people if you can't engage them in productive, respectful discussions.
➢ Be discerning with what content worth sharing.
➢ Use technology to collaborate effectively
➢ Use context-appropriate language to ensure clarity.

Reflective:
➢ Define boundaries on healthy use of technology.
➢ Define personal boundaries on how often others can communicate with you
➢ Consider what content is healthy for you to engage with online
➢ Consider the ethics of people to whom you provide a platform
➢ Consider how people's presentation can differ from their offline presentation
➢ Determine and support your best digital reputation
➢ Consider the privilege that comes with your access to technologies.

Principles:
➢ Respect laws and community guidelines
➢ Be productive and positive in your digital communities.
➢ Proactively respect other's boundaries.
➢ Utilise digitalisation where possible to reduce paper waste.
➢ Keep your privacy setting in alignment with your values.

5. Bring Your Own Device

Device Specifications

Charlton Brown College endorses laptop devices running either Apple or Windows operating systems. For convenience, Charlton Brown College has established an agreement with *The School Locker* to provide approved devices for the school – any of the devices listed on the Charlton Brown College technology page on the School Locker website will meet the required device specifications. While families are welcome to source devices themselves, we recommend visiting the above-mentioned

page first to get the specification details, including the requirement that the device is a laptop rather than a tablet.

Recommended Accessories:
All students:

> ➢ Bluetooth or USB mouse, USB flash drive
> ➢ Headphones with a microphone, which will be used where distance learning is required

ICT Costs & Software Levies

The purchase and associated maintenance costs of students' devices are the responsibility of the students and parents/guardians.

All software, access to required systems, and associated technical support are included in tuition fees. As students will be given access to Charlton Brown internet, networks and systems, students and parents should also be aware of the requirements of the Charlton Brown Internet & Network Usage Policy as it applies to students.

Damage, Loss & Maintenance

Damage, loss, and maintenance are responsibilities of the student and parent/guardian, so we advise closely reviewing warranty information before purchasing a device, as well as purchasing a carry case appropriate to the mobility and work practices of students. ***The School Locker,*** like many retailers, offers coverage packages which provides support beyond the requirements of The Australian Consumer Laws (e.g. accidental damage), which can be reviewed and purchased at the discretion of the student and parent/guardian.

General Technical Support

Charlton Brown IT staff will manage the setup of College email accounts, as well as assistance with specific software setup if required. College IT staff will provide general technical support during regular business hours via an email or live chat. Queries outside of business hours will be answered on the next business day.

6. Charlton Brown College & Social Media

Being a college comprised of a community with diverse beliefs and backgrounds, the College has a responsibility to protect its name, intellectual property, and community members. As such, in addition to the requirements of the Social Media Policy, Charlton Brown states the following advice regarding use of social media:

> ➢ Use of the College brand (including the logo, colours, official photographs, or any other intellectual property or proprietary materials) is not permitted unless prior written permission is obtained from the Principal (or approved delegate).
> ➢ Official social media accounts, statements, comments, views, etc. can only be made on behalf of the College by an approved individual.
> ➢ Information about the college not publicly available must not be disclosed.

- Images and/or recordings of College community members participating in College related events, or in identifiable College facilities or other college-branded or owned material must not be posted without prior written consent from the Principal (or approved delegate).
- When using personal accounts to comment or share content, all community members must ensure views are solely their own and must not associate themselves or their views with the college.
- Posts or content on personal social media by any College community member that could reflect badly on the college community must not be shared and may incur disciplinary action.
- The following are considered major breaches of this policy and will incur disciplinary action: cyberbullying; digital misrepresentation of oneself (catfishing); illegal sharing or use; intellectual property misconduct; publishing one's own or another's personal information/content; viewing and sharing age-inappropriate content such as explicit sexual material, pornography, and sexting; or engaging in any other digital behaviours causing harm, humiliation, or bad repute.

7. Use of Mobile Phones

Mobile phones and other digital devices have become an acceptable technological accessory for people to use to their own advantage. As in the wider society, so too this is the case increasingly in colleges.

The College recognises that there are occasions when it is genuinely appropriate and beneficial for people to have access to such devices. There are, however, occasions when the use of these devices is restricted. The College provides the following guidelines:

- Staff, parents and students are permitted to carry a mobile phone to school, at the owner's risk. The security of the mobile phone is the responsibility of the owner. College resources will not be allocated to finding a phone that is lost or allegedly stolen.
- While in the classroom, mobile phones are restricted to curriculum-related use at the discretion of the classroom teacher.
- Apple watches and other interactive devices must be switched on silent and should not be used during lesson time.
- Mobile phones must be switched off or silenced in all lessons, college gatherings and other formal college occasions.
- Mobile and smart technology are not permitted in test/examination rooms.

During lesson times, the College asks that parents contact students through reception rather than through personal mobile devices

8. Responsibilities

Student Responsibility

Students are responsible for meeting the expectations laid out in this policy by their signing of the Digital Citizenship & BYOD agreement as part of the Letter of Offer and Agreement, which are included in the enrolment process. Students should take special note that these practices extend to their personal use of social media. These practices will be reiterated in the College's Orientation program, where students (and their parents/guardians) are encouraged to seek clarity in any cases of

uncertainty. Students are responsible for the management and maintenance of their technology (e.g. school resources will not be allocated to find lost mobile phones, etc.).

Where policy infractions occur, students should take responsibility in reporting and working with IES College to action a plan appropriate to the circumstance. For major or repeated minor infractions, forms of exclusion may be used.

Staff & Community Responsibility

All staff, equally to students, are also responsible for meeting the expectations laid out in this policy. All college staff and community members should take special note that these practices also extend to their personal use of social media. The college will support students to follow this policy through education on topics such as:

- The details of this policy, and other related IT policies
- Current Australian law including cyberbullying, child abuse, accessing and sending explicit sexual material, copyright, intellectual property misconduct, etc.

Academic Director

The Academic Director (or delegate of the Academic Director) is responsible for:

- Implementing the policy across the College
- Ensuring all students and staff are aware of the Policy's contents
- Ensure that student's receive instruction in acceptable device, internet & network/systems use at the College
- Approving appropriate sharing of social media content by community members; and
- Ensuring adequate supervision of technology use in the school.

Charlton Brown IT Team

The IT team is responsible for monitoring student use of the network, ensuring appropriate network access and restrictions are applied to student access, assisting with student IT enquiries or concerns, monitoring student use of school technology, and reporting any unacceptable use to the Academic Director.

Teachers

Teachers will assist in the implementation and further development of this policy, as well as serving as examples of best practice. Teachers are responsible for building students' abilities in subject-specific technologies, as well as serving as a first point of contact in classroom-related IT issues.

Parent/Guardian

Parents/guardians are responsible for supporting holistic implementation of this policy by their signing of the Digital Citizenship & BYOD agreement as part of the Letter of Offer and Agreements, which are included in the enrolment process.

Any off campus use of personal or school technology is the responsibility of the students and student's parents/guardians. While the college employs content-filtering technology to limit the websites that may be accessed using the network, these technologies are not failsafe.

9. The Use of Third-Party Web-Based Systems

As is required of any contemporary education, the College uses many third-party web-based systems. The content and operation of these systems are not controlled by the College. The use of these websites may be governed by the third-party provider's terms of use and students must comply with such terms when using the site.

Students may be required to create a login for these websites, which will include the disclosure of their name and their College email address. Where this may be required, College staff will guide students through this process.

10. Review and feedback

This policy will be reviewed annually, and amendments and updates implemented as required. The compliance manager will communicate key changes/updates made to policy documents with relevant business units/faculties who will be responsible for disseminating that information to their staff, and where relevant, students and parent.

The college staff, student, and parents/guardians may provide feedback or inquiries about this document by contacting the compliance Manager be emailing robyn.tyler@charltonbrown.com.au

Version History				
Review Period:		2 years from date of last approval		
Version Number:	Approved by:	Approval Date:	Effective Date:	Sections Modified:
D1				New Policy developed
1.0	CEO	May 2022	May 2024	Approval of new policy

IT 8.1.01 POL Information Technology and BYOD Policy_2022_v1