St Charbel’s College’s ‘Bring Your Own Device’ program aims to improve student learning experiences both in and out of the classroom. St Charbel’s College provides considerable freedom to students in their choice of technology and the school does so with the expectation that they will make good decisions with regard to their personal use of technology.

This Bring Your Own Device Policy must be agreed to and signed before students are permitted to bring their device to school and connect it to school facilities.

Students and parents/carers must carefully read this Policy prior to signing it. Any questions should be addressed to the school and clarification obtained before the Policy is signed.

**Bring Your Own Device Policy Agreement:**

1. We have read the BYOD Policy and associated appendices.
2. We understand our responsibilities regarding the use of the device and the Internet.
3. In signing below, we understand and agree to the BYOD Policy.
4. We understand that failure to comply with the BYOD Policy will invoke the school’s standard disciplinary procedures.

<table>
<thead>
<tr>
<th>Name of Student</th>
<th>Signature of Student</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name of Parent/Carer</td>
<td>Signature of Parent/Carer</td>
<td>Date</td>
</tr>
<tr>
<td>Name of Parent/Carer</td>
<td>Signature of Parent/Carer</td>
<td>Date</td>
</tr>
</tbody>
</table>
1. INTRODUCTION AND PURPOSE

St Charbel’s College, grants its students the privilege of purchasing and using tablets and laptops of their choosing at school for their convenience and learning. St Charbel’s College reserves the right to revoke this privilege if students do not abide by the policies and procedures outlined below. This policy is intended to protect the security and integrity of the College’s data and technology infrastructure. Students of St Charbel’s College must agree to the terms and conditions set forth in this policy in order to be able to connect their devices to the College network.

The policy and procedures are to be adopted by the College from Years 7 to 12, inclusive; with the Primary School to be included within the following year.

Rationale

Information Communication Technology (ICT) will be used effectively to enhance learning and teaching in all curriculum areas, to support collaborative and co-operative learning, to develop higher order thinking skills and to help all students to realise their educational and social potential. Leveraging digital technologies to improve student learning experiences is a key part in fulfilling that mission. Many students own devices such as tablets, and laptops that can supplement their learning if used appropriately in the classroom. The purpose of the Bring Your Own Device (BYOD) initiative is to move further into the digital learning age by facilitating safe and productive use of such devices and thereby to empower students to take more active ownership of their own learning. The device becomes another tool in the learning repertoire of students.

Web-based tools and resources have changed the landscape of learning. Students now have at their fingertips unlimited access to digital content, resources, experts, databases and communities of interest. By effectively leveraging such resources, students can not only deepen their learning, but they can also develop digital literacy, fluency and citizenship that will prepare them for the high tech world in which they will live, learn and work. A device in the hands of every student through a BYOD model could extend and enrich learning by:
• Shifting teaching and learning towards more student-centred learning, where inquiry and authentic learning are emphasised.
• Focusing on contemporary learning, including critical and creative thinking, collaboration, communication, self-direction, global awareness and cultural literacy.
• Increasing student engagement.

Teachers are encouraged to facilitate the use of students’ devices in their classes where they deem appropriate. Use of students’ own devices in class is, however, at the sole discretion of the teacher. Teachers will follow standard discipline procedures in case a student fails to bring their device, in the same manner as if a student fails to bring any other required material to class.

The BYOD initiative is customisable for differing learning styles – it allows students to use different devices to customised assignments which can play off the strengths and learning styles of each student. It provides access to digital content and digital learning environments that provide multiple pathways to learning. The devices that students bring to school will allow them to connect to our own learning platform, Moodle, and the College’s learning environment. ICT allows students to make connections locally and globally that adds authenticity to school work. This enables students to learn while pursuing real-world issues and topics of deep interest to them, both individually and collectively, within their communities of interest and beyond.

If the devices the students use beyond the school day are the same ones they use for school, the students can seamlessly switch from personal use to learning anytime, anywhere. The learning activities on the device are accessible to the students 24-hours-per-day, 7-days-per-week, enabling them to pursue personal interests associated with such learning. As a result, the students are literally carrying around accessibility to academic learning that can be called up at a moment’s notice.

2. SCOPE

The document applies to all staff members and students at St Charbel’s College.

3. DEFINITIONS

“Staff member” includes:

• paid employees whether employed on a permanent, temporary or casual basis
• religious, volunteers, contractors, sub-contractors, consultants and students on tertiary practicum placements

“Student” refers to any child enrolled at St Charbel’s College.
4. LEGAL FRAMEWORK

Staff members are required to be familiar and comply with child protection legislation as varied from time to time, including but not limited to:

- Child Protection (Working with Children) Act 2012 (NSW)
- Child Protection (Working with Children) Regulation 2013 (NSW)
- Children and Young Persons (Care and Protection) Act 1998 (NSW)
- Children and Young Persons (Care and Protection) Regulation 2012 (NSW)
- Crimes Act 1900 (NSW)
- Enhancing Online Safety for Children Act 2015
- Ombudsman Act 1974 (NSW)

Failure to comply with the child protection responsibilities and obligations required by legislation or this document will result in disciplinary action being taken, up to and including immediate termination of employment, termination of contractor agreement, notification to external agencies and/or criminal charges.

A staff member who becomes aware of a possible breach of this document or legislation by another staff member must report this to their supervisor. Failure to do so may result in disciplinary action.

5. RESPONSIBILITIES AND OBLIGATIONS

Duty of care

Staff members have a legal obligation to take reasonable care for their own safety and the safety of children and others with whom they come into contact as part of their engagement with St Charbel’s College.

6. FURTHER INFORMATION

Further information about the processes outlined in this document can be sought from the Head of School or Principal.

RELATED DOCUMENTS

- Appendix A: BYOD Acceptable Use
- Appendix B: BYOD Specifications
- Appendix C: BYOD Access and Security
- Appendix D: BYOD Risks, Liabilities and Disclaimers
- Behaviour Management Policy
- Bring Your Own Device Policy Agreement
- Code of Conduct and Student Management Policy
- Communication Devices Staff and Student Use Policy
- IT User Policy
- Social Media Guidelines
- Student Use of Digital Devices Policy
Acceptable Use

- The device brought to school pursuant to this policy must be brought on every school day and be solely the student’s to use throughout the school day.

- Our College defines acceptable use as activities that directly or indirectly support the ethos and mission of St Charbel’s College. Student-owned devices are used primarily for teaching and learning in a safe and productive learning environment.

- 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.

- Whilst connected to the College’s wireless network, students are blocked from accessing certain websites during school hours. These websites are blocked and/or filtered at the discretion of the College and at the request of the College.

- Device cameras or video recording facilities are only to be used in the pursuit of learning.

- Students are not permitted to film or photograph fellow students or members of the teaching staff without receiving prior permission.

- Devices may not be used at any time to:
  - Store or transmit illicit materials
  - Store or transmit information belonging to another person
  - Harass, bully or defame other students or members of the teaching staff

- Students may use their mobile device to access the following school-owned resources: email, calendars, contacts, documents and other network resources such as Moodle.

- St Charbel’s College has a zero-tolerance policy for using the devices to bully or harass another student or a member of the teaching staff. Disciplinary action will be taken against those students who use their device to bully other students or staff.
Devices and Support

- The College recommends one of the following devices:
  - Tablets (Apple & Android)
  - Notebooks (Running any OS)
  - Chromebooks
- All the above devices will be registered on the College network.
- Connectivity issues are supported by the College IT support team.
- Devices must be presented to the College’s IT support team for proper provisioning and configuration before they can access the network.
- It is the students’ responsibility to ensure that their device is fully charged prior to their attendance at school each morning.
- Support for these devices encompasses connection issues ONLY. No other issue will be look at or resolved unless it poses a security risk to the College network.
- Student must provide any device for examination by the College if requested.

Peripherals

- Students should avoid bringing peripheral device equipment to school with the device. Peripheral equipment includes:
  - chargers
  - charging cables
  - docking cradles, with the exception of a docking cradle that includes a keyboard integrated into the peripheral
  - adapters for the connection of video output or data transfer
APPENDIX C: BYOD Access and Security

Security

- iOS devices such as iPads, and Android devices, must have an access code set.
- For their network accounts, students should use a strong password which should include a combination of upper- and lower-case letters, numbers and symbols.
- Students are not to disclose their network password or their device PIN or password to fellow students.
- Mobile devices must lock itself with a password or PIN if it is idle for five minutes.
- Students are responsible for the backing up of all data on their device. 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.

Access and Security

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.
- 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:
  - 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 emails.
spam, e.g. unsolicited advertising material.

never send or publish:

- unacceptable or unlawful material or remarks, including offensive, abusive or discriminatory comments.
- threatening, bullying or harassing another person or making excessive or unreasonable demands upon another person.
- sexually explicit or sexually suggestive material or correspondence.
- 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 College.

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.

Privacy and Confidentiality

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.

Intellectual Property and Copyright

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.
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 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.

Monitoring, evaluation and reporting requirements

Students will report:

• any internet site accessed that is considered inappropriate.
• any suspected technical security breach involving users from other schools, TAFEs, or from outside the College.

Students should be aware that:

• their emails are archived and their web browsing is logged. The records are kept for two years.
• the email archive and web browsing logs are considered official documents.
• they need to be careful about putting their personal or sensitive information in emails or on websites.
• these records may be used in investigations, court proceedings or for other legal reasons.
Risks/Liabilities/Disclaimers

- It is the student’s responsibility to take additional precautions, such as backing up email, contacts, documents and files on their device.
- **It is the student's responsibility to ensure that their device is fully charged prior to their arrival at school each morning. Bringing an uncharged device to class will be unacceptable.**
- Students should avoid bringing 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.
- It is the student’s responsibility to ensure the security of their device during travel to and from school and whilst at school.
- It is the student’s responsibility to become familiar with their chosen device and to become proficient in its use.
- Parents and students should consider whether their device requires insurance and whether specific accidental loss and breakage insurance is appropriate for the device. If insurance is deemed to be needed, it is the parent’s responsibility to ensure that all student-owned devices are adequately insured.
- In the case of tablets with 3G/4G data plans, it is the parent’s understanding that all Internet traffic through 3G and 4G telecommunications network is unfiltered and they are responsible for all costs accrued for accessing such data through the 3G or 4G telecommunication system.
- The College reserves the right to disconnect student owned devices or disable services without notification.
- Lost or stolen devices must be reported to the College within 24 hours. Students and their parents are responsible for notifying their mobile carrier or insurance company immediately upon loss of a device.
- In circumstances where a device is damaged by abuse or malicious act of another student, reimbursement may be required. 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.
- The student is expected to use his or her devices in an ethical manner at all times and adhere to the College’s acceptable use policy.
- The student and their parents are personally liable for all costs associated with his or her device.
- St Charbel’s College reserves the right to take appropriate disciplinary action for noncompliance with this policy and where a device has been used to defame, bully, or harass a fellow student or member of the teaching staff or if the device has been in such a way as to hinder the teaching and learning environment.