BRIGIDINE COLLEGE RANDWICK

STUDENT BRING YOUR OWN DEVICE (BYOD) POLICY

1. Key principles

1.1 Access to the Brigidine College Randwick (BCR) network, including the Internet, will be made available to students who bring their own devices to school for appropriate learning activities in addition to accessing resources and research materials.

1.2 Bring Your Own Device provides an effective process that allows BCR to efficiently incorporate student-owned devices into our digital learning environment while maintaining the security of school and SCS infrastructure and data.

1.3 The device in BYOD refers to any of the following technologies.
   - Laptops
   - Tablets
   - Convertible laptop/tablet

2. Registration for network accessibility

2.1 BCR will enable one device per student and provide a common platform for students to use and ensure device compliance.

2.2 All student devices will be checked and registered with BCR IT Staff.

3. Student BYOD Agreement

3.1 Prior to connecting their device to the network, students must return a Student BYOD Agreement. This agreement must be signed by the student and by a parent/carer.

3.2 Students will be made aware of and agree to their obligations under the Student Bring Your Own Device (BYOD) Policy prior to using their own device in the schools digital learning environment. School staff should endeavour to ensure that the BYOD student responsibilities are clearly understood by both students and their parents or carers.
3.3 The Student BYOD Agreement is a simple document with the purpose of acknowledging acceptance and agreement of the terms associated with the school’s implementation of the Student Bring Your Own Device (BYOD) Policy by both students and parents/carers. It is accompanied by a specifications and FAQ’s Sheet that must be provided in conjunction with the Student BYOD Agreement.

3.4 By accepting the terms, the student and parents/carers acknowledge that they:
   - agree to comply with the conditions of the Student BYOD Policy.
   - understand that both the school and SCS have the capacity to access their device and the data/information it contains at the Principal’s discretion.
   - understand that under no circumstances will SCS or the school accept any liability for the theft, damage or loss of any student’s device.
   - understand that non-compliance may result in the withdrawal of BYOD permission and access.

3.5 Student BYOD agreements should be retained in print or electronic form for future access as required.

4. Cost to Students

4.1 Access to school printers will be managed by the PaperCut printing monitoring program. Students can purchase credit to use school printers and photocopiers.

4.2 Access to the school network and provided software will be available to students i.e. SENTRAL. Parents will be expected to pay their yearly technology levy to contribute to the overall cost of providing this access.

5. Student and Parent/Carer Responsibilities

5.1 Students are solely responsible for the care and maintenance of their BYO devices. This includes but is not limited to:
   - Managing battery life and regular charging of their own device.
- Labeling their own device for identification purposes.
- Purchasing and using device protective casing.
- Ensuring the device is kept safe and secure.
- Maintaining up-to-date anti-virus software and operating system on their device.

5.2 Students are responsible for managing the battery life of their BYODs device and acknowledge that the school is not responsible for charging their devices. Students should ensure that their devices are fully charged before bringing them to school. BCR is not responsible for providing facility for students to charge their devices at school.

5.3 Student devices must meet the minimum device specifications including maintaining current antivirus software installed on their BYODs device and must continue to maintain the latest service packs, updates and antivirus definitions.

5.4 Students should not attach any school-owned equipment to their BYO devices without the permission of the school principal or their delegate.

5.5 Students should clearly label their BYOD device for identification purposes.

5.6 Students are responsible for securing and protecting their device in school. This includes protective/carry cases, ensuring the device is kept in their padlocked locker when not in use and exercising common sense when storing the device. BCR is not required to provide designated or secure storage locations.

5.7 Students are responsible for ensuring the operating system and any software on their device is legally and appropriately licensed.

5.8 Students will use their BYOD device for educational purposes only during classes and will not connect to the internet using their own internet connection (if they have one), and therefore bypass SCS web filtering, whilst on the school grounds.

5.9 Students will bring their BYOD device everyday so that they are available for educational use in all classes. Students without a BYOD will need to borrow an ex-DER laptop so that all students have access to online resources.
6. **Damage and Loss**

6.1 Under no circumstances will SCS or the school accept any liability for the theft, damage or loss of any student’s device.

6.2 In cases of malicious damage or theft of another student’s device, existing school processes for damage to school or another student’s property apply.

6.3 BCR will regularly review policies and processes to include BYO devices where appropriate e.g. Student Wellbeing and Discipline Policies.

7. **IT Support**

7.1 Students will not receive ICT hardware or software technical support from the school’s ISO for their individual BYO device.

7.2 BCR IT Staff will provide support and review BYOD devices for suitability and assist with connecting the device to the school wireless and school based software i.e. SENTRAL and Canvas

8. **Long-term care and support of BYODs**

8.1 Students and parents/carers are solely responsible for repair and maintenance of their own device. It is not the school’s responsibility.

8.2 Warranties: Students and parents/carers should understand the limitations of the manufacturer’s warranty on their BYO devices, both in duration and in coverage. Under Australian consumer legislation, warranties usually last for one year, during which any manufacturing defects will be repaired or the device will be replaced (as per the specific terms and conditions of the manufacturer).

8.3 Extended Warranties: At the time of purchase, students and parents/carers may also purchase an optional extended warranty (past the standard warranty period) from the supplier/manufacturer of their device, during which any manufacturing defects that may occur will also be repaired.
9. Insurance

9.1 Student BYO devices are not covered by the School’s Insurance Policy. When students purchase their BYO device, they may also purchase an optional insurance policy from the supplier of their device or a relevant insurance company. As mobile devices are subject to a higher risk of accidental damage, prior to signing up for an insurance policy, parents/carers should be fully aware of the details and limitations of the policy, including any excess charged for making a claim, and the name of the company that holds the policy. As a guide, a suitable BYOD device insurance policy should cover all types of BYOD devices and provide worldwide, replacement cost coverage against:

- accidental damage,
- damage from falls and liquids,
- theft
- fire
- vandalism
- natural disasters (such as floods, cyclones, earthquakes, tornados, water damage, and power surge due to lightning)

10. Acceptable use of BYO devices

10.1 Using BCR or SCS’s network services to seek out, access, store or send any material of an offensive, obscene, pornographic, threatening, abusive or defamatory nature is prohibited. Such use may result in legal and/or disciplinary action, including suspension from school.

10.2 Students shall not create, transmit, retransmit or participate in the circulation of content on their devices that attempts to undermine, hack or bypass any hardware and software security mechanisms that have been implemented by, SCS’s, or BCR.

10.3 Students must not copy, transmit or retransmit any material that is protected by copyright, without prior permission from the copyright owner.

10.4 Students must not take photos or make video or audio recordings of any individual or group without the express written permission of each individual.
(including parent/carer consent for minors) being recorded and the permission of an appropriate staff member.

10.5 Students shall comply with SCS’s and/or school policies concerning their use of BYODs device at school and while connected to SCS’s network including:

- Online Communication Services – Acceptable Usage for School Students.

10.6 The principal retains the right to be the final arbiter of what is, and is not, appropriate use of BYO devices at BCR within the bounds of NSW privacy legislation.

10.7 The consequences of any breaches of this policy will be determined by the principal, in accordance with the school’s Welfare and Discipline Policy.

11. Device Minimum specifications

11.1 Prior to purchasing or using an already purchased device, parents and students should be made aware of the following technology standards required for devices at BCR:

- SCS wireless network installed in at BCR only operates on the 802.11n 5Ghz standard. Devices with 802.11a/b/g or 802.11n 2.4Ghz only will not be able to connect.
- The battery life of the device should be capable of lasting 6 hours minimum of constant use without charge.
- Device must have a physical keyboard for typing (on-screen keyboards reduce screen visibility and are generally harder to operate.
- Device must have a 10 inch screen or larger.
- Device must have a HTML5 web browser installed.
- Device must have up to date anti-virus software installed.

11.2 Other considerations when purchasing a device include:

- Extended warranty
- Device insurance
- Protective casing (scratch/impact/liquid-splash resistant)
- Additional or spare battery packs
- Ergonomics (is this device comfortable to use for an entire school day)
- Backup storage such as portable hard drive or USB flash drive
12. Security and device management processes

12.1 The network will become the point where SCS’s and BCR’s security policies are implemented.

12.2 There are a wide range of security considerations that will be addressed. These include but are not limited to:
- Strong passwords
- Device anti-virus software
- Data and network traffic encryption
- Privacy controls
- Internet filtering
- Student Cyber Safety

12.3 Educational policies and security processes will be updated as required to ensure a secure and effective digital learning environment.

This policy should be read and interpreted in conjunction with:
- Copyright Law of Australia
- BYOD Acceptable Use Agreement
- BYOD Agreement Form
- BYOD Specifications
- BYOD Warranty FAQ’s
- BYOD Laptop Loan Agreement
- SCS’s Acceptable Use Policy