Introduction: This document provides guidance and direction to principals, staff and school communities for the management of the Student Bring Your Own Device (BYOD) Policy.

1. Key principles

1.1 Access to the Sydney Girls High School (SGHS) 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 SGHS to efficiently incorporate student-owned devices into our digital learning environment while maintaining the security of school and Departmental infrastructure and data.

2. Registration for network accessibility

2.1 SGHS 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 SGHS IT Staff.

3. Student BYOD Agreement

3.1 Prior to connecting their device to the network, students must return their Student BYOD Agreement. This agreement must be signed by the student and by a parent/carer. The principal may accept the student’s signature for students living independently.

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 school’s digital learning environment. School staff should endeavor to ensure that the BYOD student responsibilities are clearly understood by both students and their parents or carers.

3.3 The purpose of the Student BYOD Agreement is for both students and parents/carers to acknowledge and accept the terms associated with the school’s implemented Bring Your Own Device (BYOD) Policy.

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 set out in this document.
   • Understand that both the school and the Department have the capacity to access their device and the data/information it contains at the Principal’s discretion.
3. Understand that under no circumstances will the Department or the school accept any liability for the theft, damage or loss of any student’s device.

4. **Cost to Students**

4.1 Internet access through the Department’s network will be provided at no cost to students in NSW Public Schools.

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

4.3 Parents will be expected to pay their yearly technology levy. This is used to contribute to the overall cost of providing access to the development, installation, and implementation of computer systems and applications including educationally required hardware, software and IT Service Desk support staff.

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 should ensure that their devices are fully charged before bringing them to school. Students are responsible for managing the battery life of their device and acknowledge that the school is not responsible for charging their device.

5.3 The student’s device must meet the minimum device specifications including maintaining current antivirus software installed on their 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 device without the permission of the school principal or their delegate.

5.5 Students are responsible for securing and protecting their device at school. This includes protective/carry cases and exercising common sense when storing the device. Schools are not required to provide designated or secure storage locations.

5.6 Students are responsible for ensuring the operating system and any software on their device is legally and appropriately licensed.
5.7 Students will use their device for educational purposes only during classes.

5.8 Students are not to connect to the internet using their own personal connections, therefore bypassing the Department web filter whilst on the school grounds; this includes the use of Personal Hotspot via their mobile phone.

5.9 Students will bring their 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 from the IT Office so that all students have access to online resources.

6. Damage and loss

6.1 Under no circumstances will the Department or the school accept any liability for the theft, damage or loss of any student’s device. Please refer to:

The Use of mobile phones, portable computer games, recording devices and cameras in schools and TAFE NSW institutes


Claims for loss of or damage to personal property and use of private motor vehicles by staff, parents and students


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

6.3 SGHS will regularly review policies and processes to include BYO devices where appropriate e.g. Student Welfare and Fair Discipline Code.

7. IT Support

7.1 Students will not receive ICT hardware or software technical support from the NSW Department of Education for their individual BYO device.

7.2 SGHS IT Staff will provide support and review BYOD devices for suitability and assist with connecting the device to the school wireless and virtual desktop environment.

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 Treasury Managed Fund. 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 SGHS 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 the Department, its Information Technology Directorate or SGHS. This includes the use of personal hotspots.

10.3 Students should ensure that their devices are fully charged before bringing them to school. They 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 departmental or school policies concerning their use of their device at school and while connected to the Department’s network including:

• Online Communication Services – Acceptable Usage for School Students.
• Acceptable Use of Department’s portal services.
10.6 The principal retains the right to be the final arbiter of what is, and is not, appropriate use of BYO devices at SGHS 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. **Security and device management processes**

11.1 The network will become the point where Departmental security policies are implemented.

11.2 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
- Departmental antivirus
- Departmental technology infrastructure security
- Student Cyber Safety

11.3 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:

- [Code of Conduct Policy](#)
- [Copyright Law of Australia](#)
- [Values in NSW Public Schools](#)
- [Department of Education and Training Privacy Code of Practice](#)
- [Online Communication Services – Acceptable Usage for school students](#)
- [Legal Issues Bulletin No. 35 November 2012](#)
- [Legal Issues Bulletin No. 8 September 2012](#)
- [Online Communication Services: Acceptable Usage for School Students](#)