# BRING YOUR OWN DEVICE (BYOD) POLICY

**Purpose**

Pittwater High School is committed to providing supportive learning environments for all students and is keen to assist students with personal devices (laptop / tablet). Clearly, safety and security from both the student's point of view and the school's are prime concerns as is the impact on school resources. Consequently, the following policy position has been established.

**Policy**

Students, parents and guardians must read and understand these guidelines and sign the contract agreement before a student can connect a BYOD device to the school's network and internet services. If a student connects a device without a user agreement they are in breach of the school rules and subsequent discipline action will be taken. PHS reserves the right to confiscate any unauthorised device. The School adopts this policy in order to maintain a safe and secure environment for students and its staff.

A personally owned device shall include all existing and emerging technology devices that can take photographs; record audio or video; input text; upload and download media; and transmit or receive messages or images, and with internet capability. Examples of a personally owned device most suited to a wide range of learning activities shall include but is not limited to: an ipad or other tablet, a laptop or netbook computer, as well as any device with similar capabilities.

1. BYOD can only be used at school with the knowledge and written approval of the parent/guardian and Pittwater High School. The signing and returning of the **BYOD User Agreement Form** constitutes such knowledge and approval. Students should be able to show a **PHS BYOD sticker** on their device.
2. The student's name should be clearly visible on the back of the device and should not be able to be easily removed.
3. Student takes full responsibility for his or her device and keeps it with them at all times. PHS is not responsible for the security of the device.
4. Students are responsible for the proper care of their personal device, including any costs of repair, replacement or any modifications needed to use the device at school.
5. Student devices are not covered by NSW Treasury Managed Fund. The student accepts FULL responsibility for the care and use of their own device. In particular, the school does not accept responsibility for theft or loss of the device or parts/accessories. Families should check the details of their personal insurance coverage for events such as loss/damage. Unless specifically stated Home and Contents insurance does not cover a device against accidental breakage or theft when outside the home. There is risk associated with bringing a device to school and it is highly recommended that parents consider electing to purchase a suitable insurance option as part of their Home and Contents package. Devices should be transported in protective cases specifically designed for that device.
6. Under no circumstances are students to leave a device unattended. This includes occasions when undertaking extra and co-curricular activities. Students must always take home their devices overnight and never leave them in a locker.
7. Students should always attempt to minimise the total weight of materials transported to and from home. Remember that the device is valuable and always have it in sight or preferably hold it when travelling.
8. PHS reserves the right to inspect a student's personal device if there is reason to believe that the student has violated any Department of Education policies, administrative procedures, school rules or has engaged in other misconduct while using their personal device. Violations of any school policies, administrative procedures or school rules involving

a student's personally owned device may result in the loss of use of the device in school and / or disciplinary action.

9. The device will only have access to the school's wireless network. Students will still be bound by the Technology and Network Policy Contract which is signed by every student at the beginning of each year.
10. At NO stage will students have direct access to the Pittwater High School server. The integrity of the Pittwater High School network could be severely compromised by the introduction of viruses and this is a risk that cannot be accepted.
11. Via the wireless network students will have access to the school's learning management system (Moodle), the filtered Internet and the DEC Student Portal.
12. Students must be aware of appropriateness of communications when using school or personally owned devices. Inappropriate communication is prohibited in any public messages, private messages, and material posted online by students.
13. Students are not permitted to use any device to record audio or video media or take pictures of any student or staff member without their permission. The distribution of any unauthorised media may result in disciplinary action including but not limited to suspension, criminal charges, and expulsion.
14. Students may not utilise any technology to harass, threaten, demean, humiliate, intimidate, embarrass, or annoy their classmates or others in their community. This is unacceptable student behaviour known as cyber bullying and will not be tolerated. Any cyber bullying that is determined to disrupt the safety and/or well being of the school is subject to disciplinary action.
15. PHS attempts to provide a safe Internet experience for students by deploying state of the art filtering technology. If students use 3G or 4G this will not apply.
16. When at school, students will use their wireless connection exclusively for educational purposes. Activities such as; downloading files not related to schoolwork, playing computer games or watching movies is not permitted.
17. The use of a device at particular times in individual lessons is at the **discretion and direction of the teacher**. There may be times when the activity is intended to be completed without device assistance or when the attention of the student is required elsewhere. At NO stage should students access programs or material from the device that are not relevant to their current work or learning. In the event of students using their device inappropriately, the teacher may require the student to close down the computer and continue working via other means.
18. Students are expected to bring their devices to school each day with a fully charged battery.
19. Students should not attach any school-owned equipment to their mobile devices without the permission of their supervising teacher.

**Technical Assistance or Advice**

The school cannot undertake to provide technical assistance for hardware or software problems that may occur with devices. Such assistance remains the personal responsibility of the student as a private matter. If the device malfunctions during a lesson, the student is required to continue with their learning promptly in a conventional manner.

20. The student is responsible for ensuring that any software or application required is already installed on their device. The school is unable to supply or install software due to resource constraints and licensing agreements. Where specific software is required for classroom learning and or tasks, the teacher will provide access to the software via desktop computer in one of the computer labs at school.
21. Students are encouraged to perform regular backups of their files. The importance of current work will often determine back up frequency. PHS is not responsible for any data loss. Under the school's Assessment Policy, loss of data is not a valid excuse for the late submission of a task.
22. Printing of documents from student devices can only be done through school desktop computers using a **personal data-transfer device (USB) compatible with the school network**

**computers**. Direct connection of the device to the printer network is not permitted. It is the student's responsibility to have a suitable data-transfer device.

23. The use of a device at school is regarded as a privilege and teachers may wish to view the work being carried out on the device during class time. Students are required to provide the teacher with access to the device to view the school related files when asked. Where there is reasonable suspicion that material contrary to the ethos of the school is being brought to school or accessed during class time on the device, the school reserves the right to impound the device and institute a search for such material.

**Security**

System security is protected through the use of passwords. Failure to adequately protect or update passwords could result in unauthorised access to personal or school files. Each user is required to report any security problems to the PHS technical support staff in Library. The problem is not to be demonstrated to other users. To protect the integrity of the system, the following guidelines shall be followed:

24. Users shall not reveal their passwords to another individual.
25. Users are not to use a device that has been logged in under another user's name.
26. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the network.
27. Users are required to have an appropriate **anti-virus software installed on their devices** to avoid any spread of virus on the school network. Students are also responsible to update their anti-virus software on a regular basis.
28. Students should use strong passwords and have suitable privacy controls.
29. Students will need to complete a new BYOD agreement in order to add a new device if their previous devices are no longer in use.

**Intellectual Property and Copyright**

Students will:

30. Never plagiarise information and will observe appropriate copyright clearance, including acknowledging the author or source of any information used.
31. Ensure that permission is gained before electronically publishing users' works or drawings. Always acknowledge the creator or author of any material published.
32. Ensure any material published on the internet or intranet has the approval of the principal or their delegate and has appropriate copyright clearance.
33. Never copy, transmit, retransmit or download any material that is protected by copyright, without prior permission of the copyright owner.
34. Ensure that the operating system and all software on their device are legally and appropriately licensed.

**Pittwater High School Technology Standards**

35. The school's Wi-Fi network installed operates on the 802.11n 5 GHz standard. **Devices that do not support this standard will not be able to connect.**