Jamison High School

222 Evan St, South Penrith 2750

T: 4731 6150 F: 4721 2502
jamison-h.school@det.nsw.edu.au
www.jamisonhighschool.nsw.edu.au

JAMISON HIGH SCHOOL
INFORMATION COMMUNICATION TECHNOLOGY (ICT) AND
BRING YOUR OWN DEVICE (BYOD) POLICY

Terms

BYOD: Bring Your Own Device refers to the program whereby students are permitted to bring a form of technology that is capable of connecting to the school's wireless network to support their learning at school. There are conditions and standards defined in the BYOD Policy.

Device: Refers to technology that students bring from home to connect to the school wireless network in the BYOD program.

ICT: Information Communication Technology is technology such as computers and the necessary enterprise software, middleware storage and audio-visual systems that enable users to access, store, manipulate and transmit information. This applies to, but is not limited to, use of school's hardwired and wireless network and the use of personal devices that utilise other networks in order to transmit data, the use of cloud based resources and the use of portable storage devices.

Purpose

Jamison High School, (JHS) is committed to providing an engaging learning environment for all students and is keen to support students with personal laptops/tablet devices. Safety and security, from both the student's and school's point of view, are prime concerns, as is the impact on school resources. Consequently, the following Policy Position has been established.

Policy Guidelines

Students need to be aware of and read the:

Communication Services: Acceptable usage for School Students and the Jamison High School **ICT/BYOD Policy** that you are currently reading.

The DoE's Communication Services: Acceptable usage for School Students can be found at:
https://education.nsw.gov.au/policy-library/policies/online-communication-services-acceptable-usage-for-school-students?refid=285859
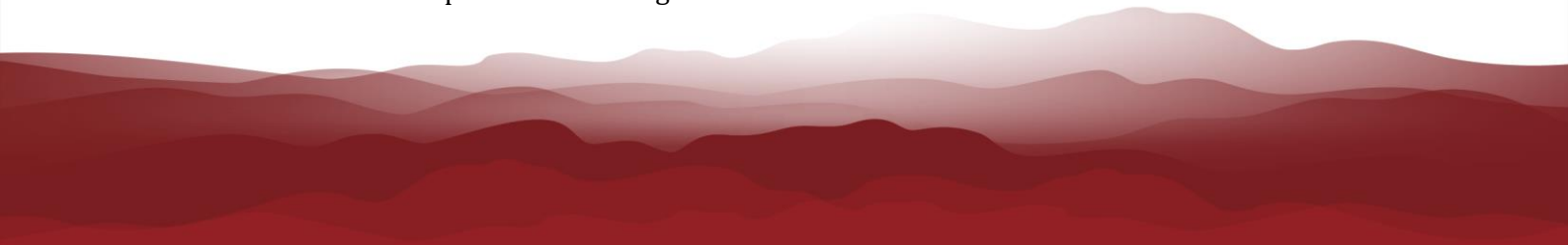
The DoE's BYOD Policy can be found at:
https://education.nsw.gov.au/policy-library/policies/student-bring-your-own-device-policy-byod?refid=285859

> **Students and parents/guardians must read and understand these guidelines before students are permitted to connect a BYO Device to the school's wireless network services. It is mandatory that all policy guidelines are followed. In cases of breach of school rules and policies, disciplinary action may be taken. JHS 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. Examples of devices include but is not limited to: iPads, Kindle, and other tablet PC's; laptop and netbook computers;

Laptop computers (or tablet devices) can only be used at school with the knowledge and written approval of the parent/guardian and JHS. The reading of the **ICT/BYOD User Agreement Form** constitutes such knowledge and approval.

1. The student's name should be clearly visible on the back of the device and should not be able to be easily removed.
2. Students must take full responsibility for his/her device. JHS is not responsible for the security of the device.
3. Students are responsible for the proper care of their device, including any cost of repair, replacement or any modifications needed to use the device at school. The school does not accept responsibility for **theft or loss of the device** or parts and accessories. Families are strongly encouraged to arrange suitable insurance cover for such loss/damage (Unless specifically stated Home and Contents insurance does not cover a laptop/device against accidental breakage or theft when used outside the home.
4. Devices should be transported in protective cases specifically designed for that device.
5. Students should always attempt to minimise the total weight of materials transported to and from home. For this reason we have specified devices with a smaller form factor.
6. JHS reserves the right to inspect a student's personal device if there is reason to believe that the student has violated any DOE policies, administrative procedures, school rules or has engaged in other misconduct while using their personal device. Any violations involving a student's personal device may result in the loss of the use of the device in school and/or disciplinary action.
7. Student must be aware of the appropriateness of communication when using school or personally owned devices. Inappropriate communication is prohibited in the form of any public messages, private messages and material posted online by students. Students must not utilise any technology to harass, threaten, demean, humiliate, intimidate, embarrass or annoy their classmates or others in their school community. This unacceptable behaviour, known as cyber bullying, will not be tolerated and will be subject to disciplinary action.
8. Students are not permitted to use any electronic 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.
9. JHS attempts to provide a safe internet experience for students by deploying DoE's filtering technology. To utilise the school's wireless network students are required to log in through their DoE Student Portal. As most mobile phones can be used to access the internet, bypassing the DoE filtering, these will not be allowed to use as personal devices under the JHS ICT/BYOD Policy.
10. When at school, students will use their wireless connection exclusively for educational purposes. Activities such as downloading files not related to schoolwork, playing games or watching movies is not permitted and contravenes acceptable use of the school wireless network and may result in disciplinary action.
11. The use of a laptop/device at particular times in individual lessons is at the discretion of the teacher. There may be times when the activity is intended to be done without computer assistance or when the attention of the student is required elsewhere. At NO stage should a student access programs or material from the laptop/device which are not relevant to their current work/learning. In the event of students using their laptop/device inappropriately, the teacher may require the student to close down the computer and continue working via other means.
12. Students are expected to bring their devices to school each day with a fully charged battery. There will be no provision to charge batteries at school.

13. Students should not attach any school-owned device/ equipment to their mobile devices without the permission of their supervising teacher.

Technical Assistance or Advice

JHS provides some basic technology assistance through ICT support staff. The support is limited to ensuring that the device is connected to the wireless network and some basic troubleshooting relating to network connectivity. However, the school cannot undertake to provide technical assistance for hardware or software problems that may occur with laptops/tablet devices. Such assistance remains the personal responsibility of the student as a private matter. If the laptop/tablet device malfunctions during a lesson, the student is required to continue with his learning promptly in a conventional manner.

14. The student is responsible for ensuring that any software or application required is already installed on their laptop/tablet 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 labs at school.

15. Students are encouraged to perform regular backups of their files. The importance of current work will often determine backup frequency. JHS is not responsible for any loss of data. It should be noted that loss of data is not a valid excuse for the late submission of a task. Students are encouraged to increasingly utilise cloud based options for backing up data (Google Drive/OneDrive).

16. Currently, printing of documents form student laptop/tablet devices can only be done through the school desktop computers using a USB device, by storing and accessing the data from a cloud based storage location or by emailing the information to themselves. Direct connection of the laptop/tablet device to the printer network is not permitted. It is the student's responsibility to have a suitable USB drive.

17. The use of a personal laptop computer at school is regarded as a privilege and teachers may wish to view the work being carried out on the computer during class time. Students are required to provide the teacher with access to their personal device to view the school related work files when asked. Where there is a reasonable suspicion that material contrary to the ethos of the school is being brought to school or accessed during class time on the personal laptop/tablet device, the school reserves the right to impound 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 JHS technical support staff. The problem is not to be demonstrated to other users. To protect the integrity of the system, the following guidelines shall be followed:

18. Users shall not reveal their passwords to another individual.

19. Students who are also enrolled with TAFE or have a TAFE account are not permitted to use TAFE logins at school. This will be considered as breach of the User Agreement and may result in disciplinary action.

20. Users are not to use a computer or network resource that has been logged in another user's name.

21. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the network.

22. Users of BYOD are required to have appropriate anti-virus software installed on their devices to avoid the spread of viruses. This software will also need to be kept updated with the latest definitions.

23. Students should strong passwords and have suitable privacy controls. Applications such as https://howsecureismypassword.net/ can be used to check password strength.

Intellectual Property and Copyright

Students will:

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

Jamison High School Technology Wi-Fi Standard

29. The schools' Wi-Fi network operates on the **802.11n 5GHz Dual Band**. Devices that do not support this standard will not be able to connect.