



BYOD POLICY 2022

Internet Acceptable Use Guidelines

Wentworthville Public School is committed to future focused learning through the integration of technology into all teaching and learning programs. A broad range of technology tools are used every day to enhance quality learning experiences for students and to explicitly teach the skills required to be digitally savvy in an increasingly technologically reliant global community. It is important to remember that the device you bring to school does not replace workbooks, written activities, and other learning endeavours. The device is one of many learning tools used to enhance educational experiences.

Access to Wentworthville PS network is a privilege, not a right. The use of technology, whether owned by Wentworthville PS or devices supplied by the student, requires personal responsibility. It is expected that students will comply with Wentworthville PS rules regarding Internet use furthermore act in a responsible manner and will honour the terms and conditions set by the classroom teacher additionally Wentworthville PS school executives. Failure to comply with such terms and conditions may result in temporary or permanent loss of access to school network as well as other disciplinary or legal action as necessary. Students will be held accountable for their actions and are encouraged to report any accidental use immediately to their classroom teacher or school administration.

Network Guidelines

1. Personal Safety

- a. Students should not reveal personal information including names, addresses, photographs, credit card details or telephone numbers of themselves. They should ensure that privacy and confidentiality is always maintained.
- b. Students will not agree to meet with someone they have met online without parental approval.
- c. If a student believes they have received unsolicited email, or they have received a message or other online content that is inappropriate or makes them feel uncomfortable, they must inform their teacher, or other school employee as soon as is possible.

2. Illegal Activities

- a. Students will not attempt to gain unauthorised access to Wentworthville PS network resources or to any other network to go beyond their authorised access. This includes attempting to log in through another person's account or access another person's files. These actions are illegal, even if only for the purposes of "browsing."
- b. Students will not make deliberate attempts to disrupt the school network or destroy data by spreading computer viruses or by any other means. These actions are illegal.



Telephone: 9631 8529
9631 8492

Fax: 9896 3079

- c. Students will not read, move, rename, edit, delete, or in any way alter the files that have been created or organised by others.
- d. Students will not install or alter software or hardware on any school computers.
- e. Students will not create, participate in, or circulate contents that attempt to undermine, hack into and/or bypass the hardware and/or software security mechanisms that are in place or breach the department's network security.
- f. Even where consent is obtained for recording, the school will not tolerate images or sound captured by personal technology devices on the school premises or elsewhere being disseminated to others. If it is done for the purpose of causing embarrassment to individuals or the school, for the purpose of bullying or harassment, including racial and sexual harassment, or where without such intent a reasonable person would conclude that such outcomes may have or will occur.

3. Security

- a. Students are responsible for their individual accounts and should take all reasonable precautions to prevent others from being able to use their account.
- b. Students will immediately notify a teacher if they have identified a possible security problem with the network. They will not go looking for these security problems, because this may be considered an illegal attempt to gain access.
- c. Students will take all precautions to avoid the spread of computer viruses.
- d. Students are not allowed to bring in 4G and 5G wireless connections. To ensure that our school network is not compromised and that students are not able to access an unfiltered internet connection whilst at school.

4. Inappropriate Language

- a. Restrictions against inappropriate language apply to public messages, private messages, and material created for assignments or to be posted on web pages.
- b. Students will not use inappropriate language in any correspondence.
- c. Students will not use the school network to engage in bullying or harassment. If a student notices anyone engaging in such behaviours they will immediately notify a teacher.



- d. While at Wentworthville PS, students have access to a Department of Education, Training and Employment email account, which they can access from home and school for the purposes of learning. Email traffic is monitored for inappropriate use, content and language.

5. Respect for Privacy

- a. Students will not invade someone's privacy by taking unauthorised personal photographs or recording personal conversations; including the further distribution (e.g. forwarding, texting, uploading, Bluetooth use etc.) of such material.
- b. Students will not repost a message that was sent privately or post private information about another person.
- c. Students will not utilise another student or staff member's username or password to access the school's network, including not trespassing in another person's files, shared drive or email.

6. Respecting Resource Limits

- a. Students will use the technology at the school only for educational activities.
- b. Students will not post chain letters or engage in "spamming." Spamming is sending an annoying or unnecessary message to a large number of people.
- c. Students will not download or use games, applications, pictures, video, music, instant messaging, e-mail, or file sharing applications unless they have direct authorisation from a teacher. Use of Department of Education/school networks to upload files to cloud based storage is prohibited, such as but not limited to i Cloud, Drop box, Onedrive etc.
- d. Students understand that staff will monitor and access any equipment connected to the Wentworthville PS network, resources and their computer activity.

7. Plagiarism and Copyright Infringement

- a. Students will not plagiarise work that is found on the Internet or on the computers at school. Plagiarism is taking the ideas or writings of others and presenting them as if they were their own. Copying of software, information, graphics or other data files may violate copyright laws without warning and be subject to prosecution from agencies to enforce such copyrights.



Telephone: 9631 8529
9631 8492

Fax: 9896 3079

- b. Students will respect the rights of copyright owners. Copyright infringement occurs when a student inappropriately reproduces a work that is protected by a copyright. Students will appropriately reference sources for any school assignments.

8. Inappropriate Access to Material

- a. Students will only access audio/videos files, websites and programs that relate to their educational activities. Students will not be permitted to use the internet at Wentworthville PS to download non- learning related audio/video files, website content, programs and iTunes content,
- b. Students will not use the school network resources to access or store material that is inappropriate.
- c. If students mistakenly access inappropriate information, they will immediately tell a teacher and will not attempt to access the inappropriate information again.
- d. Parents will instruct their child if there is additional material that they think would be inappropriate for them to access. The school fully expects that students will follow their parent's instructions regarding this matter.

STUDENT BRING YOUR OWN DEVICE (BYOD)

GUIDELINES

1. Access to the department's Wi-Fi network and resources

- 1.1 Internet access through the department's Wi-Fi network will be provided on departmental (Department of Education) sites at no cost to students who are enrolled in NSW public schools.
- 1.2 Access to school resources such as shared drives, printers and associated costs will be a school-based decision.
- 1.3 Wentworthville PS will provide information in relation to student access and usage of its network and reserves the right to restrict/remove student access to the intranet, extranet, internet or network facilities if parents or students do not adhere to the school's network usage and access guideline/statement.
- 1.4 Wentworthville PS will educate students on cyber bullying, safe internet and email practices and health and safety regarding the physical use of electronic devices. Students have a responsibility to incorporate these safe practices in their daily behaviour at school.

Telephone: 9631 8529
9631 8492

Fax: 9896 3079

2. Acceptable use of devices

- 2.1 Students must comply with departmental and school policies concerning the use of devices at school while connected to the department's Wi-Fi network.
- 2.2 Students should not attach any school-owned equipment to their mobile devices without the permission of the school principal or staff member.
- 2.3 Students must 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 the school.

- 2.4 Students must not copy, transmit or retransmit any material that is protected by copyright, without prior permission from the copyright owner.
- 2.5 Students must not take photos, make video or audio recordings of any individual or group without permission of staff.
- 2.6 Students and their parents/caregivers must be advised that their activity on the Internet is recorded and that these records may be used in investigations, court proceedings or for other legal reasons.
- 2.7 Students must not store, display or access inappropriate images on any personal devices whilst on school premises.

Where staff has reasonable grounds to suspect that a device contains data which breaches the BYOD Student Agreement, the principal may confiscate the device for the purpose of confirming the existence of the material. Depending on the nature of the material involved, school disciplinary action may be appropriate or further action may be taken including referral to the police.

The consequences of any breaches of the school's BYOD policy will be determined by the principal in accordance with relevant Department policies and procedures and accepted school practice

3. BYOD Student Agreement

Schools must ensure that students and their parents/caregivers are aware of, and agree to their obligations under the school's BYOD policy and other relevant departmental policies.

- 3.1 Prior to connecting their devices to the department's Wi-Fi network, students must return a BYOD Student Agreement.
- 3.2 The BYOD Student Agreement contains both BYOD Device Requirements and BYOD Student Responsibilities.

Telephone: 9631 8529
9631 8492

Fax: 9896 3079

- 3.3 By accepting the terms of the BYOD Student Agreement, the student and parents/caregivers acknowledge that the student:
- 3.4 agrees to comply with the conditions of the school's BYOD policy; and understands that noncompliance may result in disciplinary action.

We will retain a copy of the BYOD Student Agreement in print or electronic form and it will be kept on file with the student record.

4. Long-term care and support of devices

Students and their parents/caregivers are solely responsible for the care and maintenance of their devices.

- 4.1 Students must have a supported operating system and current antivirus software installed on their device and must continue to maintain the latest service packs, updates and antivirus definitions as outlined on the BYOD Student Responsibilities document.
- 4.2 Students are responsible for ensuring the operating system and all software on their device is legally and appropriately licensed.
- 4.3 Students are responsible for managing the battery life of their device. Students should ensure that their devices are fully charged before bringing them to school. Schools are not responsible for providing facilities for students to charge their devices.
- 4.4 Students are responsible for securing and protecting their device in schools, and while travelling to and from school. This includes protective/carry cases and exercising common sense when storing the device. Devices will be locked in a storeroom or cupboard when the class is not in their room. Devices are not to be used in the playground or on the trip to and from school.
- 4.5 Students should clearly label their device for identification purposes. Labels should not be easily removable.
- 4.6 Students should understand the limitations of the manufacturer's warranty on their devices, both in duration and in coverage.

5. Damage and loss

- 5.1 Students bring their devices onto the school site at their own risk
- 5.2 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.

Telephone: 9631 8529
9631 8492

Fax: 9896 3079

6. Technical support

Schools are under no obligation to provide technical support for hardware or software. Schools may choose to provide this service to students if there are sufficient resources available in the school.

7. Insurance

Student devices are not covered by Treasury Managed Fund. Insurance is the responsibility of parents/caregivers and students.

Please fill in the following and **return this page only** to the class teacher. Only students who have completed and returned their Internet and BYOD Acceptable Use Agreement may participate in the BYOD program.

STUDENT BRING YOUR OWN DEVICE (BYOD) Agreement

I/we have carefully read the Student Bring Your Own Device (BYOD) Guidelines and have discussed these with our child. I/we are aware of the responsibilities and appropriate use of devices at school.

Signed:

Student Name: _____

Class: _____

Student signature: _____

Date: _____

Parent signature: _____

Date: _____