ACCEPTABLE USE POLICY (AUP)

CANBERRA SECONDARY SCHOOL

[STUDENT GUIDE]

Table of Content

Introduction

In an ever-changing world, the use of Information and Communications technology (ICT) has become an integral aspect of society. Canberra Secondary School taps on Information and Communications technology (ICT) as a teaching and learning tool which fosters the development of our students' key digital skills so that they can be proficient in their use of ICT.

Nonetheless, it is a priority that the school's lessons and activities are conducted in a manner where unnecessary distractions or disruptions are prohibited. Therefore, it is necessary that students use technology, including their Personal Learning Devices (PLD) such as laptops/tablets/mobile phones responsibly, ethically and respectfully of others in an appropriate manner which is consistent with the School's Standard Operating Procedures and Acceptable Use Policy. Consideration must be given at all times to the possible effects of one's actions when using technology at school or at home.

It is our goal to empower our students to make their PLD/Internet experiences safe and responsible. The school teaches Online Safety as part of the Character and Citizenship Education (CCE) lessons to educate students on how to avoid dangerous, inappropriate, or unlawful online behaviour. Cyber wellness matters are also communicated during Year Head Cohort talks and CCE lessons.

The aim of this Responsible Use of Technology is to ensure that students will benefit from learning opportunities offered by the school's Internet resources in a safe and effective manner. Internet use and access is considered a school resource and privilege.

Thus, it is our vision that all three key stakeholders, the school, parents and students, collaborate in this mission to create an engaged and effective learning environment that better equips our students for the 21st century.

Standard Operating Procedures for Using Computing Device

1. Use of Computing Device (Access)

1. During curriculum time, devices are to be used only during lessons or when working on tasks/activities assigned by the teachers. Students will need to stay on relevant sites and be on task when working on any activities with their devices at all times.

2. When teachers need to get attention from the students, they will need to turn over their devices and ensure that the screens are facing down. Students are to adhere to the following:
    - 'Screens down': Put the screen facing down and pay full attention to the teacher
    - 'Screens up' : Continue with the learning activity on device

3. When working on activities that involve audio such as watching videos, students will need to use their personal earpieces or for those without, they will need to set the volume to an appropriate level that do not disrupt others.

4. When Personal Learning Devices (PLD) require connection to the internet, students are to ensure that the Wi-Fi of their devices are switched on and connected to pdlp@SSOE.

5. For any password issues such as not being able to access school wireless network, students can inform their Character Coaches (CCs), alert the ICT manager or report using the online Request form provided on the school's website.

6. For any password issues with SLS, it is the students' responsibility to resolve the issues soonest. They are required to perform a password self-reset where possible first, failing which, they can report using the online Request form provided on the school's website.

7. Students are to use the online Request form provided on the school website to report any device fault.

2. Use of Computing Device (Security)

1. CCTVs are installed in every classroom for greater security.

2. Every classroom is equipped with a metal cabinet for storing devices and the class chairperson/vice-class chairperson will sign out/in the cabinet key from the General Office. Only the chairperson/vice-class chairperson who sign out the keys can open up the metal cabinet to keep/retrieve devices in/from the cabinet. The chairperson/vice-class chairperson must not pass the key to any of his/her classmates.

3. Students should always bring their devices and accessories (such as the keyboard and Apple pencil) with them when leaving their classrooms for lessons in other venues. However, students should keep their devices and accessories in the metal cabinet provided in the classroom and lock them up when going for recess. When devices are not in use and students are not leaving their classrooms for recess, students must keep the devices and accessories in their bags and not leave them in the open such as on the tables. Students are allowed to purchase their own anti-theft security holder and lock to secure their devices to the table if needed. At the end of the school day, students are required to bring their devices home and not leave any devices in the metal cabinet.

4. Similarly, for students who are attending CCA after school, they are required to store their devices in the CCA metal cabinets provided at the CCA venue before going for their CCA. At the end of the CCA session, they are required to bring their devices home and not leave any devices in the metal cabinet. Only assigned CCA student leaders of each CCA are allowed to draw out the keys from the general Office.

5. For outdoor learning with the devices, students are required to exercise due diligence to look after their devices and accessories, and not leave them unattended or unsupervised. The devices and accessories should be stored in their school bags where possible.

6. Students should form the habit of checking frequently and ensuring that the PLD are kept with them or locked up in the metal cabinet at all times. Any PLD that is seen lying around such as on the tables when the whole class is not in the classroom will be picked up and passed to the Operations Manager in the General Office for safe-keeping. Students are required to collect the devices back from the Operations manager at 4.30pm on each day.

7. For any loss of device, students are to report to their CCs or subject teachers **immediately** who will then alert the Operations Manager. The school will advise the next course of action such as making a police report if necessary.

3. Use of Computing Device (Management)

1. Each student's device will be installed with a Device Management Application (DMA) in 3 different areas by default to help in managing the devices. For in-school use of the PLD, schools will have the autonomy to manage the default settings and operate the DMA solution, based on the baseline policies that MOE HQ provide:

    1. Mobile Device Management - Allow for central administration of the personal learning devices to ensure consistent remote deployment of applications as well as security patches.
    2. Usage Management – Restrict the type of apps and websites accessible by the students and limit the amount of screen time through technology.
    3. Classroom Device Management - Enable teachers to actively monitor and control the

students' screens in class.

2. Students are required to hold their devices securely with their hands when handling the devices/moving from one location to another.

3. Students are not allowed to charge their devices in the classroom which includes charging their devices due to low battery after curriculum usage. They are responsible for charging their devices at home everyday. Students should ensure that their personal device is fully charged before bringing it to school.

   i. For contingency situations such as students on FAS and who do not have the means to charge at home, students may be allowed to charge their devices using the powerpoints in the library or any charging stations set up in the school.

Emergency loan of school-owned devices

4. For students who forget to bring their devices, they can loan school-owned devices for that day. School-owned device can be a chromebook or tablet depending on the availability.

5. The students will go to the library (Computer Lab 1) and look for Ms Jacqueline Koh or Desktop Engineers (DEs) to sign out their devices before the flag-raising at 7.50am and return the devices at the end of the school day at 3.30pm.

6. Students must return the devices by 3.30pm and not later such as after their CCA to minimise the risks of losing the devices/theft/mishandling the devices.

7. Students are not allowed to bring the loaned devices home.

8. Students must remember to bring their devices as part of their responsibility for learning. The ICT manager will keep track of students who forget to bring their devices and loan out school-owned devices. On the second time that the students loan out the device, the ICT manager will alert the CCs so that they can follow-up with the student and inform parents on student's responsibility to bring their PLD to school. Repeat cases will result in referral to Year Head and possible disciplinary action. In such cases, school discipline measures and consequences apply.

Acceptable Use Policy (AUP) Agreement

It is the intent of the Canberra Secondary School to advance and promote education by assisting in the collaboration and exchange of information. Successful operation of Internet and other related technological services requires that all students regard the system as a shared resource. Students must cooperate to form a community of diverse interests with a common purpose of advancing education. It is, therefore, imperative that all students conduct themselves in a responsible, ethical, and polite manner.

In order to ensure a safe and conducive learning environment, students are to abide by the rules stated in this Acceptable Use Policy Agreement.

This policy applies to all students in this school and their usage of our school's ICT facilities, equipment, and resources, as well as students' personal devices (e.g. mobile phones/tablets/laptops). ICT facilities, equipment, and resources include the following, but are not limited to, the school's internet network, IT Lab, hardware (e.g. laptops, tablets, computers), software (e.g. school's learning management system, productivity software, online tools) and peripherals (e.g. projector, scanner, camera).

General

1. Students are responsible for their personal learning devices (PLD). Although the PLD that students are getting under the MOE bulk tender comes with a 1-year insurance coverage that includes 1 repair or 1 replacement, students shall note that accidental loss is not covered by the insurance.

Insurance Coverage	**Claimable**
● Fire ● Lightning ● Power Surges ● Accidental e.g water spillage, drop etc ● Theft due to forcible entry ● Robbery* *Accidental loss will not be covered by insurance	1 repair or 1 replacement (1-year insurance)

2. The school will not be held responsible for any damage, theft or loss of their devices. In the event of loss or theft of devices, students must report the matter to the school immediately.

3. Students shall bring their PLD home with them at the end of every school day.

4. Students shall not use the school's electrical power to charge their own personal devices. Students should ensure that their personal devices are fully charged before bringing them to school.

5. Students' PLD are installed with Device Management Application (DMA). When enrolled, the software will manage students' device usage based on settings selected. Students should not attempt to uninstall or de-enroll themselves from the software. Any violation might lead to disciplinary action in accordance with the school's discipline policy.

6. Students are only allowed to use their devices when working on school related activities or doing school work. Students are not allowed to use their devices to engage in inappropriate activities such as online chats, watching irrelevant video clips and playing games even during recess and lunch breaks.

7. Students shall not use their devices to store, modify or create content (e.g. documents, presentations, pictures, videos) that is pornographic or defamatory in nature.

8. Students shall not use their devices for any online trade (i.e. buying and selling of goods and services).

9. Students are responsible for using school-owned ICT facilities, equipment and resources for the purpose of learning.

10. Students are responsible for any resource that is borrowed from school for the duration of the loan. The student will bear the cost of damage, theft or loss due to negligence and face disciplinary action in accordance with the school's discipline policy.

Account

11. Students are responsible and accountable for all activities conducted via their own account(s), including logging in to the school's wireless network for internet access.

12. Students are responsible for the security of their account IDs and passwords. All account IDs and passwords should not be shared with anyone.

13. Students shall change their passwords every 90 days.

14. Students are to use their full name as stated in their EZlink cards for all account IDs. Aliases, nicknames and pseudonyms are not allowed.

15. Students shall not use their accounts for any illegal or unethical activities. These include posting online remarks that are racially and religiously insensitive, vulgar and/or offensive statements, disruptive of public order and intentionally causing emotional distress/harm to others.

16. The school reserves the right to record and retain data on school-owned devices and/or accounts issued by the school for investigation or evidence.

17. Network administrators may review files and communications to maintain system integrity and ensure that the system is used responsibly.

18. Violation of any policies, rules or administrative procedures may result in a temporary suspension or revocation of the student's account. The student may also face disciplinary action in accordance with the school's discipline policy.

Email, Internet and Social Media

19. Students are to exhibit positive online behaviour, practise safe and responsible use of their devices, and be respectful of self and others at all times.

20. Students shall be responsible for all content that they upload, post, email, transmit or otherwise make available via the school network.

21. Students shall not upload or download, send or post, enter or publish any content on the internet that is objectionable or illegal under the Singapore Law.

22. Students shall not post or share any content on the internet that is against the public interest, public order, national interest, racial and religious harmony, or which offends good taste or decency, or is otherwise indecent, obscene, pornographic or defamatory.

23. Students are reminded that threats, harassment, embarrassment, impersonation and intimidation to others are chargeable offences under the Singapore Legal System.

24. Students shall be mindful of the public nature of the internet and shall not discuss or disclose confidential and proprietary information of the school or any organisation.

25. Students are expected to remain courteous and polite in all online interactions.

Privacy and Safety

26. Students shall be respectful of all staff and students and their rights to privacy.

27. Students shall be mindful of the need to protect their own privacy. Students should not expect that data stored in social media platforms or email servers are private.

28. Students shall not reveal their personal details (e.g. phone number, home address, NRIC, passwords, or passwords of other people) openly online.

29. Students shall be discerning when accessing websites. They shall avoid websites of unknown or disreputable origin.

30. If students inadvertently access a website that contains obscene, pornographic, or otherwise

offensive material, notify a trusted adult (e.g. parents or teachers) immediately.

31. Any attempt to alter data, the configuration of a computer, or the files of another student, without the consent of the individual, is an act of vandalism and subject to disciplinary action in accordance with the school's discipline policy.

32. School will use DMA to blacklist known sites that are inappropriate and track students who are browsing undesirable sites.

Intellectual Property

33. Students shall not access, download, copy or share any copyrighted materials (such as pictures, videos, music) without explicit permission from the owner.

34. The rights of all materials and data created using the school's ICT facilities and resources are jointly owned by the school and the student.

35. Student's work may be considered for publication on the World Wide Web, specifically on the school's Website or a classroom Website.

Software

36. Students shall not own, copy, install or share software in an unauthorized or illegal manner.

37. Students should install anti-virus software for PLD that require the protection. However, anti-virus software is unnecessary for iPads due to the unique design of its operating system.

Contacts

Canberra Secondary School
Tel: 6758 5070
Fax: 6758 3110
canberra_ss@moe.edu.sg

For Technical Helpdesk
Ms Jacqueline Koh
(ICT Associate Manager)
62571915
koh_mei_fang_jacqueline@moe.edu.sg

For PDLP/ICT Inquiry
Mr Goh Ching Tard
(HOD ICT)
Ext: 117
goh_ching_tard@moe.edu.sg