XMS ICT ACCEPTABLE USE POLICY (AUP) 2026

(XMS IT AUP Agreement For Use Of Edtech Resources)

Purpose of the Acceptable Use Policy (AUP)

Technology is an essential part of learning in today's world. This Acceptable Use Policy (AUP) establishes guidelines on the appropriate use of EdTech resources to help students understand how to use these resources safely and responsibly, in line with efforts to develop digital literacies and growth as digitally responsible citizens.

EdTech resources include the following, but are not limited to:

- Learning devices (e.g. Personal Learning Devices (PLDs), school devices, IT lab devices)

- ICT system accounts (e.g. Singapore Student Learning Space (SLS), iCON, Student MIMS, school Google account)

- School internet networks and school/MOE digital services

For more information, please refer to:

- Student Kit on Cyber Wellness and Learning with a Learning Device (Primary): https://go.gov.sg/cw-studentkitpri

- Student Kit on Cyber Wellness and Learning with a Personal Learning Device (Secondary): https://go.gov.sg/cw-studentkit

Introduction and Scope

Computing devices and internet access have become essential for work, recreation, and education. As you engage with the digital realm, it is imperative to do so responsibly and safely. The school is dedicated to creating a secure and supportive environment for your learning experience. As a user of the school's IT facilities and resources, you are expected to adhere to the guidelines outlined in this **Acceptable Use Policy Agreement (AUP).**

This policy applies to all enrolled students of the school and encompasses their use of learning devices, IT lab facilities, equipment, and IT resources beyond the school's site. It also extends to the school's internet network, both MOE and school-deployed IT system accounts, hardware (e.g., laptops, tablets, computers), software (e.g., Device Management Application (DMA), productivity software, online tools), and peripherals (e.g., projector, scanner, camera). Users should exercise care during use to reduce wear and tear on any hardware in school.

Non-compliance with this AUP may result in disciplinary action in accordance with the school's discipline policy.

A. Personal Learning Device (Your Chromebook / PLD)

1. You are accountable for your Personal Learning Device (PLD). Only school approved devices can be used. Do not use your personal windows-based notebook or tablet. If the device is lost or stolen, it is your responsibility to file a police report and inform the school.

2. Ensure your PLD is fully charged before bringing it to school. Make it a habit to charge your Chromebook every evening. If you need to charge it during the school day, you may only do so at the school's designated charging point(s) (e.g. the charging kiosk in the library), during recess and/or after-school hours, unless otherwise instructed by the school.

3. Your device comes equipped with a Device Management Application (DMA) to support a safe and conducive learning environment and allow appropriate internet connectivity. Do not attempt to uninstall the DMA, bypass it, or de-enrol the PLD from it. The school will periodically check DMA enrolment and may issue warnings and/or take disciplinary action for non-compliance. All lessons in class that uses the PLD will be regulated via the DMA Content Management System by your Subject Teachers. Please adhere to this protocol.

4. Unauthorised access to data, systems, and information is strictly prohibited. You should not attempt to access resources that you are not authorised to. Do not attempt to visit banned websites via the school internet provision.

5. You are reminded that the use of PLDs and the school's EdTech resources is solely for the purpose of learning. Do not abuse this privilege.

6. Keep your PLD updated by installing relevant patches and updates when prompted or when instructed by the school.

7. You are responsible for regularly backing up your learning materials in your PLD (e.g. to your school Google Drive) to prevent data loss.

8. If you suspect your PLD is malfunctioning, please visit the IT service desk in the library between 9.00 am to 11.00 am on usual curriculum school days. The desktop engineers will inspect and advise you on the next step.

B. General Use of School ICT Facilities and Resources

9. Utilisation of school-owned ICT facilities, equipment, and resources is strictly reserved for educational purposes. Activities like light gaming and engaging in social media platforms should be kept to a minimum and must not affect your learning. Such activities should not be conducted during lessons.

10. You bear the responsibility for any IT resources borrowed from the school, including costs related to damage, theft, or loss due to negligence. Disciplinary action, as per the school's discipline policy, may be taken.

11. The security and well-being of personal devices lie within your responsibility, with the school assuming no liability for any damage, theft, or loss. You are advised to secure your Chromebook/phone (e.g. lock in lockers) if they are not required.

12. School-owned computing devices and/or school/MOE accounts are not to be used for online trading or commercial activities (buying and selling of goods and services).

C. Accounts and Passwords

13. You bear responsibility and accountability for all activities conducted through your accounts.

14. School accounts include: Student MIMS, SLS, school Google account, MOE-Students iCON.

15. You must safeguard your account IDs and passwords and must not share them with others. Set up necessary authentication where required.

16. Regular password changes every three months are encouraged for good security practices. Passwords should fulfil the criteria of sufficient length and a mixture of alphanumeric characters, symbols, and uppercase characters.

17. If you have forgotten your password, you can click on the password reset link on the <Helpdesk> link under the <Resources for Parents & Students> page on the school website.

18. You should not share your MOE/school email accounts freely for non-educational websites/purposes as these can be used for spamming activities. Be careful in the use of your XMS or iCON email addresses when signing up on platforms, unless instructed by your teacher.

19. You are warned to avoid illegal or unethical activities through your accounts (e.g. cyber-bullying, posting insensitive remarks, disrupting public order, or intentionally causing distress to others).

20. Do take note that your PLD is monitored through DMA. Please do not use it to create, modify, store, or share pornographic, obscene, indecent, defamatory, or otherwise inappropriate content.

D. Being a Responsible Digital Citizen (Online Conduct)

21. You should interact with others in a respectful and responsible way. You should not post online remarks that are:

   - racially and/or religiously insensitive,

   - vulgar and/or offensive, or

   - hurtful to others.

22. You should not use any devices or accounts to:

   - store, modify, create, or share content (e.g. documents, presentations, pictures, videos) that is inappropriate (e.g. indecent, pornographic, defamatory, hurtful to self or others),

   - make threats, cause harassment or embarrassment, impersonate, or intimidate others.

23. Users are expected to adhere to netiquette (internet behaviour rules) and maintain a courteous and polite demeanour in all online interactions. Engaging in threats, harassment, embarrassment, impersonation, and intimidation online may be a chargeable offence under Singapore law.

E. Respecting Copyright and Intellectual Property

24. You are reminded to obtain explicit permission from the content owner(s) before downloading, copying, editing, or sharing any copyrighted materials (e.g. pictures, videos, music). Credit must be given to the source material if used for educational settings.

25. Unauthorised ownership, copying, or sharing of software and digital files is strictly prohibited.

26. The rights to materials and data created using the school's ICT facilities and resources may be jointly owned by the school and the user, where applicable.

F. Using Artificial Intelligence (AI)

27. You must ensure that you meet the minimum age requirement specified in each AI tool's age restrictions before using it.

28. If the use of AI is permitted for learning tasks, you should acknowledge the use of AI in weighted assessments and homework as required by your teacher/school guidelines.

29. You are to practise academic integrity and be responsible for your own learning when using AI. You are ultimately short-changing yourself if you pass off others' work (including AI-generated work) as your own.

30. You should exercise caution regarding the limitations of AI tools, including potential inaccuracies or fabricated responses, inherent biases, and outdated information.

G. Staying Safe and Secure Online

31. You should report any incidents (e.g. unusual device behaviour, suspected compromise of accounts, or inappropriate use of devices) to the school as soon as possible.

32. Develop online safety habits. This includes:

   - not disclosing personal access credentials (e.g. MIMS password, PLD passcode) to anyone,

   - not sharing sensitive personal data (e.g. home address, passwords) online or on AI platforms,

   - verifying the credibility of online content before sharing,

   - avoiding clicking on suspicious links or downloading unknown files,

   - being cautious when interacting with others online (e.g. on social media) and not engaging with strangers.

H. Digital Wellbeing and Balance

33. You are reminded to balance screen time with other activities including physical exercise and face-to-face social interactions.

34. Avoid excessive use of devices outside learning hours.

35. Take regular breaks to rest your eyes and mind.

36. Practise good sleep hygiene by not using your devices one hour before bedtime.

I. Photography and Videography at School Events / Publication of Students' Work

37. The school reserves the right to capture photographs or video images of users or their parents/legal guardians during school activities.

38. Selected images or recordings may be used and published in school communications, publications, website, and social media channels. Parents/legal guardians may opt out by providing written notification to the school.