Canadian
International
School

www.cis.edu.sg

Lakeside Campus
7 Jurong West St 41,
Singapore 649414
P. +65 6467 1732
lakesidecampus@cis.edu.sg

CIS Acceptable Network Use Policy (ANUP).

1. INTRODUCTION - The Canadian International School (CIS) has a responsibility to protect the School and its Information Technology (IT) resources from illegal or damaging actions.

2. The term “Users”, as used in this ANUP includes both staff and students unless otherwise stated as staff or students only.

3. The term “School IT resources”, as used in this ANUP includes any item that adds to, connects to, or uses the CIS Network infrastructure. This includes, but is not limited to, administrative and academic applications, computer accounts, computer equipment, cameras, databases, dial up, digital portfolios, disk storage, email, email accounts, the Internet, learning blogs, the learning management system, network, newsgroups, online discussion forums, projectors, public folders, servers, software, subscriptions, workstations, any form of digital communication, etc.

4. Participation in a community of networked computers and Users require adherence to an ethical code of conduct not unlike society at large. The fact that an activity is technologically possible does not legitimize its use. The School provides IT resources for the shared and responsible use by members of its community who are, in turn, expected to use them in an efficient, ethical, professional, and legal manner consistent with the School’s objectives, values and Singapore Law.

5. PURPOSE - The IT resources at CIS support the educational, instructional, research, and administrative activities of the school and the use of these resources is a privilege. Consequently, it is important for users to behave in a responsible, ethical, and legal manner.

   This ANUP is designed to provide an outline of appropriate and inappropriate behavior for users of the Information Technology resources at the Canadian International School.

6. APPLICABILITY - This ANUP applies to all users of the school’s IT resources - this includes staff, students, and guests. It also applies to personally owned computers and devices connected to the campus network by any means.

7. CIS reserves the right to amend this ANUP and/or implement additional policies on a regular basis. CIS will inform all users of policy changes as they occur.

8. Updated policies can be found on the school’s website. Users are responsible for staying informed about CIS policies via the school website.

9. General Provisions

9.1. Users have the responsibility to utilize the School IT Resources in a manner consistent with the mission and vision of CIS.

9.2. Files created by individual users should not be modified in any way without obtaining prior permission to do so from the file’s owner(s). Accessibility to a file does not construe consent.

9.3. School IT resources (as listed in item 3) are intended for professional use only. All materials created using School IT resources remain the property of CIS. Using School IT resources for personal usage is not permitted.

10. General Prohibited Use

10.1. Illegal Activities

Users will not engage in any activity employing School IT Resources that will be in violation of the laws of Singapore, in particular (but not limited to), the Computer Misuse Act (Cap 50A), Copyright Act (Cap 63), Spam Control Act (Cap 311A) and Undesirable Publications Act (Cap 338).

Examples include the following:

10.1.1. Downloading, distribution, sharing or storing of seditious or other materials that is likely to cause feelings of enmity, hatred, ill-will or hostility between different racial or religious groups.

10.1.2. Downloading, distribution, sharing or storing of obscene or pornographic materials or other materials depicting sex, horror, crime, cruelty, violence or the consumption of drugs or other intoxicating substances that is likely to be injurious to the public good.

10.1.3. Downloading, making copies, distribution or sharing of any copyrighted materials or intellectual property without prior permission from the copyright owner.

11. Commercial Use

Users are allowed to utilize the CIS network for commercial activities, which are defined as engaging in the provision or acquisition of goods or services for the school’s operations. Commercial use for personal consumption is not permitted

12. System Integrity

Users must not undermine or attempt to undermine the security of the School’s IT Resources in any manner. Users should not tamper with any of the School’s IT Resources that may potentially cause performance degradation, service instability, or compromise operation efficiency, security and fair use of those resources.

CIS Wi-Fi is the only network connection allowed while students are on campus. Students may not connect to any external data network via 3G, 4G, or 5G for any purpose whatsoever, whether school-related or personal. The ban on mobile data usage on campus will help any user stay secure and safe online in the school's learning environment.

13. Unauthorized Use

13.1. Users will not access or attempt to access any IT Resources to which they have not been given access including but not limited to other user’s files or school software.

13.2. Users will not access or attempt to access any data or communications not intended for them.

13.3. Files created by individual users should not be modified in any way without obtaining prior permission to do so from the file's owner(s). Accessibility to a file does not construe consent.

14. Downloading Large Files

Users will not indiscriminately download large files that may potentially consume a large amount of network/Internet bandwidth and IT Resources resulting in potential degradation of the systems for other users.

15. Proprietary/Confidential Materials

Users must keep in strict confidence any data, which is proprietary and/or confidential to the School, and use such data responsibly. Disclosure to any external party is prohibited without prior authorization in accordance with the School's policies.

16. Personal Responsibility

16.1. Users should not reveal their login and/or email passwords to anyone. Passwords should be nontrivial and changed on a regular basis.

16.2. Users will keep their ID cards secure and report any loss immediately.

17. Password Policy

Creating a strong and effective password policy for CIS IT systems is crucial to ensure the security of sensitive data and protect against unauthorized access. The password configuration listed below should be followed as closely as possible in the CIS IT systems to minimize the risk of accounts being compromised and getting hacked.

17.1. Password Complexity:
a. Passwords must be at least 10 characters long.
b. Passwords must include a mix of uppercase and lowercase letters.
c. Passwords must contain at least one numeric digit.
d. Passwords must include at least one special character (e.g., !, @, #, $, %, etc.).
e. Passwords should not contain easily guessable information, such as names, birthdates, or common words.

17.2. Password Expiry:
a. Passwords should expire every 90 days, requiring users to reset them.
b. Systems that have Multi-Factor Authentication like 2FA will have password expiry in 180 days.

17.3. Password History:
Users cannot reuse their last 5 passwords to encourage regular password updates.

17.4. Account Lockout:
After 5 consecutive failed login attempts, an account should be locked for a period of 30 minutes to prevent brute force attacks.

17.5. Password Recovery:

Implement a secure password recovery process that may involve security questions or email verification.

17.6. Multi-Factor Authentication (MFA):
All users are required to enable the MFA to add an extra layer of security if the system provides an MFA option.

17.7. Network Connections

17.8. Users will refrain from connecting any computer equipment to any wiring point whether that point is currently in use or not.

17.9. Users should not share any wireless keys, certificates or passwords they have been given.

18. Software Licenses

18.1. Users may not use or install unlicensed software or programs. Users will not infringe the copyright of any software available over the School network.

18.2. Users will comply with contractual obligations and terms and conditions of use as stated in any software licenses acquired by the School.

18.3. Software purchased by the School is Academic licenses. These licenses may allow for use at home or other locations on non-School owned computers. Users will discontinue use and un-install all school software from non-School owned computers when they leave the school, or are notified of the termination of the software license agreement.

19. Email

19.1. Email addresses on the school's mail system are assigned to all users (Grade 3 students are restricted to communication within CIS domain only).

19.2. Email is used extensively for communications and collaboration within the school community.

19.3. Users will not email or transmit defamatory, threatening or abusive messages or any messages that may be reasonably construed as such.

19.4. Users will not send annoying, abusive or unwanted messages to others.

19.5. Users will not send unsolicited mass emails, except for purposes specific to the functions and purposes of the School, or which have been approved by the Head of School.

19.6. Users will not forward messages containing general appeals or warnings like "virus warnings", "request for help‟, by mass mail or otherwise.

19.7. Users will not forge the identity of or impersonate another person in an email.

19.8. Users will not knowingly transmit by email any harmful or malicious content (e.g. viruses) or any other content or material that may otherwise violate the civil and criminal laws of Singapore.

19.9. Users will not misuse mailing lists to flood an individual, group or the email system with numerous or large emails.

20. Digital communication

20.1. With the advent of technology, increasingly sophisticated digital communication platforms are used extensively at CIS for all users. Such platforms include but are not limited to the learning management system, email accounts under the school's domain, video accounts, learning blogs and digital portfolios, where settings are controlled by users.

20.2. Users shall use the information and technology accessible through these platforms legally, appropriately and responsibly. Users shall utilize these platforms for school activities purposes only. Under no circumstances shall users engage in cyberbullying. Users also undertake not to post, publish or display any defamatory, inaccurate, abusive, obscene, profane, racially offensive, sexist or illegal material.

21. System Access

Conditions of Access

The School respects privacy and recognizes its critical importance in an academic setting. As such, the School does not, in general, intend nor wish to access Users‟ data except in the following limited circumstances:

21.1. For identification or diagnosis of systems or security vulnerability and problems in order to preserve the integrity of the IT Resources.

21.2. Where there are reasonable grounds to believe that a violation of law or a breach of the School's policies may have taken place, and such access, inspection or monitoring may produce evidence of such violation or breach.

21.3. Where specifically allowed or required under the laws of Singapore.

22. In the above situations, the School or its representatives may access all aspects of the IT Resources (excluding User owned computers), without User consent. Consistent with privacy interests of the Users.

23. Consistent with privacy interests of the Users, School access without the consent of the User will occur only with the approval of the Head of School or Director of Operations.

24. Use of Security Scanning Systems

Users consent to the School's use of scanning programs for security purposes at system and network level for computers and systems that are connected to the School's network. This is to ensure that any computers or systems attached to the network will not become a launching pad for security attacks and jeopardize the IT Resources. System level scanning includes scanning for security vulnerabilities and virus detection on email attachments.

25. Enforcement Procedures

25.1. Complaints/Reports of Alleged Violations

Any User who believes that the security of their computer account has been compromised or is aware of a violation of this Policy must report the matter to the Head of IT, who will investigate the allegation and submit a report of the alleged violation of CIS ANUP to the respective division Principals and the Director of Operations for further action.

25.2. Disciplinary Procedures

Violations of this Policy will be pursued in accordance with the appropriate disciplinary procedures for students, faculty and staff.

25.3. Network Connection and Computer Account

In the event that the situation poses an immediate security threat to the IT Resources or other external systems and jeopardizes the reputation, properties or other interests of the School, the School may disconnect the User's computer or any IT equipment from the School's network or disable their computer account for further pending actions and notify the User accordingly.

26. Legal Liability for Unlawful Use

26.1. In addition to School disciplinary actions, Users may be subject to criminal prosecution, civil liability or both for unlawful use of any of the IT Resources.

26.2. Users are reminded that unauthorized access to, modification or interception of computer programs or data can amount to serious criminal offences under the Computer Misuse Act (Cap 50A) and general law.

27. Channel of Recourse

Any User who suspects that the School or its representatives have made unwarranted access to his or her computer systems may feedback his or her concerns to the Head of School and/or Director of Operations, who will investigate the issue.

28. Care and Return of the School IT Resources

28.1. User has the responsibility to exercise due care in handling and use of the School IT Resources and agrees to return the School IT Resources in good condition.

28.2. In the event of any damage to the School IT Resources at any time while it is in the user's possession, user agrees to inform the appropriate CIS staff members (currently, any members of IT support) so that repairs can be performed on the School IT Resources.

28.3. Users are responsible for any damage to the School IT Resources due to addition or removal of software, or usage of the School IT Resources with incompatible software or hardware.

28.4. User agrees to pay for any reasonable cost of repair or replacement of the School IT Resources caused by the user's lack of care, negligence (resulting in damage or theft) or misuse.

28.5. Users will return the School IT Resources in good condition at the end of the contract period, upon terminating the employment contract with CIS.

29. Indemnity

Failure by Users to observe this Policy may result, whether directly or indirectly, in the School being involved in claims and/or suffering damages, losses and expenses.

The User will indemnify the School and its officers from any such claims, damages, losses and expenses resulting from the User's failure to observe any of the provisions of this Policy.

30. Consent to Disclosure of Information - In addition, the User must understand that the School will cooperate in any official investigations resulting from any breach of this Policy and may, in its discretion, furnish the relevant authorities/ parties with the relevant information and User’s consent to any such disclosure will be deemed by acceptance of this Policy.

I have read and accept the ANUP as stated above:

Staff Signature: ________________________________

Staff Name: ___________________________________

Date: ____