Australian Islamic College of Sydney

Acceptable Use of Computer & ICT Facilities School Policy

PURPOSE

The Australian Islamic College of Sydney (AICS) Computer Network is established for the educational and professional use of AICS students, faculty, and staff ("Users"). This Technology and Acceptable Use Policy (the "Policy") is intended to govern Users with respect to Intranet and the Internet. In addition to this Policy, AICS regulates access to and use of the Intranet by principles consistent with the educational mission of the AICS, and the rules and expectations published elsewhere (i.e., Student Diaries and Faculty Handbook). Users are expected to conduct themselves on the Intranet in the same fashion as they do elsewhere in the community.

The Intranet provides access to the global Internet. AICS has taken available precautions to restrict access to controversial materials on the Internet. However, on a global network, it is impossible to control all materials. AICS believes that the valuable information and interaction available on the Internet far outweighs the possibility that Users may find material that is not consistent with our educational goals.

The smooth operation of the Intranet relies upon the proper conduct of all Users. The signature on the Handbook Acknowledgement form are legally binding and indicate the parties who have signed have read the terms and conditions of this Policy carefully and understand their significance.

SCOPE

This document is applied to the entire Information Security Management System (ISMS) scope, i.e. to all systems, equipment, facilities and information used within the ISMS scope.

The Intranet includes all hardware, software, network services and cloud services by the AICS community, including third party services that act as extensions of our internal network.

APPLICABLE TO USERS

The target audiences for this policy are all those who use the systems and those who are responsible for managing and maintaining the information systems and infrastructure mentioned in the scope.

However, the responsibility for its implementation lies with the ICT Service Desk Team. Specifically, this process has the following audience in the organization:

a) Application administrators;
b) System Administrators;
c) Network Administrators;
d) Users for the information systems mentioned above

Users of this document are teaching staff, non-teaching staff, administration staff and students.

POLICY

1.1 Privileges

The use of the Intranet is a privilege, not a right. The use of an account must be consistent with the educational objectives of AICS. The ICT department will deem what is inappropriate use and will refer any such conduct to AICS Management. AICS, in its sole discretion, reserves the right to determine what conduct constitutes a violation of this Policy, and the discipline for any such violation. In addition, use of any other Internet connected resource must comply with the rules appropriate for that resource.

Transmission of any material in violation of any Australian regulation is prohibited. This includes, but is not limited to, material protected by copyright, threatening or obscene material, or material protected by trade practice. Use of the Intranet for commercial activities, product advertisement, or political lobbying is prohibited. Use of the Intranet and the Internet must be consistent with this Policy and all policies and practices of AICS.

1.2 No Expectation of Privacy

AICS routinely monitors usage of Intranet/Internet and may review any communications on its systems. AICS is able to override all passwords. Users do not have a privacy right in the contents of their computer system, including messages sent, received, or stored on the email systems or in their use of the Internet. Passwords to these systems exist for the benefit of AICS. Users should have no

expectation that the ability to choose a password for a system in any way limits the ability or right of AICS to monitor all activity.

1.3 Security

Security on any computer system is a high priority, especially when the system involves many Users. No User may have access to another's files on the Intranet. The following guidelines will help maintain Intranet security:

a) If you feel you have identified a security problem on the Internet, you must notify the ICT Department.
b) Do not allow anyone else to use your account and do not use another individual's account.
c) Inappropriate attempts to access a server as an administrator will result in immediate cancellation of User privileges and/ or discipline.
d) Any User identified as a security risk or having a history of problems with other computer systems may be denied access to the Intranet/Internet.

1.4 Inappropriate Access

Not all of the information freely available on the Internet is reliable or helpful. Students and employees must evaluate the source of the information, as well as the information itself, to determine its appropriateness and usefulness.

In addition to providing information, the Internet is capable of providing the means to communicate directly with others via "instant or private messaging" programs, video conferencing programs, and other means. Also, there are many places and software technologies that will allow for the free exchange of files between computers over the Internet, such as email. Not all of these methodologies are appropriate for an educational environment as outlined in this document.

Downloading or loading of software on AICS's computers is prohibited. There is an enormous quantity and variety of free software available on the Internet. However, widespread downloading of such software on the School's computers has a cumulative negative effect, and can result in the substantial degradation of performance, additional maintenance time, and increased threat of virus infestation. Students may not use school computers to access any Internet site or sites that contain information that is inappropriate for educational purposes or sites that teachers, staff or administration deem inappropriate for the instructional program. Examples of inappropriate information and/or content include, but is not limited to, the following:

Students may not access, upload, download, transmit, display or distribute:

a) offensive material – content that is in poor taste or could be considered obscene; abusive or sexually explicit language, racist, illegal, harassing or inflammatory.
b) distribute dangerous material – content that provides direction in the construction of explosives or similar devices or instruction or practices that could injure the students themselves or others.
c) inappropriate contacts – materials that can lead to contact with strangers who could potentially threaten the student's health or safety.

If a student is uncertain as to whether or not a site's material might be considered

inappropriate, the student should consult their teacher or the ICT team for clarification.

1.5 Office 365 for Education Acceptable Use

Office 365 for Education is primarily for educational use. Students may use Office 365 for Education for personal use subject to the restrictions below and additional school rules and policies that may apply.

a) Privacy

The ICT department has access to student email for monitoring purposes. Students should have no expectation of privacy on the Office 365 for Education system.

Limited personal use - Students may use Office 365 for Education tools for personal projects but may not use them for:

a. Unlawful activities.
b. Inappropriate sexual or other offensive content.
c. Threatening another person.
d. Misrepresentation of AICS staff or students.

a) Safety

a) Students will tell their teacher or the ICT Department about any message they receive that is inappropriate or makes them feel uncomfortable.
b) Students are responsible for the use of their individual accounts and should take all reasonable precautions to prevent others from being able to use their account.
c) Under no conditions should a user provide his or her password to another person.

b) Access Restriction - Due Process

Access to Office 365 for Education is considered a privilege accorded at the discretion of AICS. AICS maintains the right to immediately withdraw access and use of Office 365 for Education when there is reason to believe that violations of law or school policies have occurred. In such cases, the alleged violation will be referred to the respective Head of Schools for further investigation and account restoration, suspension, or termination. As a party of the Agreement with Microsoft, AICS also reserves the right to immediately suspend any user's account suspected of inappropriate use. Pending review, a user account may be terminated as part of such action.

Due to the rapidly changing technology environment, AICS reserves the right to determine if an action not listed in this document is inappropriate, and the student may be subject to discipline.

1.6 Managed Devices / Hardware

Students must always be assigned a device against their name during any ICT related activity which include but are not limited to classwork, research, assignments, projects etc. Students are responsible for any damage on the devices assigned against their name.

School owned devices are managed in order to allow for student use of systems only for educational purposes. Under no circumstances is a

student to attempt to modify the existing hardware configuration. Modification can be considered either opening the case or changing hardware or software settings.

It is specifically set forth in this policy that under NO circumstances are either students, staff or visitors allowed to connect their own personal computers, cell phones or any other electronic device to any of AICS computers or to the AICS internal network, without the expressed knowledge and written consent of the AICS Senior Executive (Head of School or Principal) and the ICT team or his/her designee.

AICS Information Technology offers a Wireless Network connection purposes for staff, students (year 7-12) and visitors.

1.7 Plagiarism

Information obtained from the Internet as part of a research project must be attributed to its source, using a standard bibliography notation. Students and staff may not violate a copyrighted source, or otherwise use another person's intellectual property without his or her prior approval or proper citation.

1.8 Contact

Each student and employee are responsible for all activity that occurs under his/her user account. Students and employees may not place information on the Internet that would fall under the category of "unacceptable sites" listed above.

Students may not give out any personal information (e.g., address, phone number, user name, passwords, etc.) about themselves or about other people. Students may not use school computers for commercial purposes or political lobbying.

1.9 Users are strictly prohibited from:

This is a list of the more common things students, faculty and staff are specifically NOT permitted to;

a) Download any files, especially music and videos, from the Internet, unless the material is free for commercial use and royalty free.
b) Use any form of "instant or private messaging" software on school owned devices.
c) Install any applications or software onto AICS computers.
d) Disable or modify any running tasks or services.
e) Transfer and/or store music files from any personal devices to AICS systems.
f) Play games, unless directed to by an instructor or supervisor for educational purposes, at any time on AICS computers, including Internet-based games.
g) Use proxies or other means to bypass the content filtering systems in place and or defeat any settings that prevent the access of material deemed and flagged as inappropriate by the blocking devices.
h) Use remote accessing software or hardware to take control of any network attached device or workstation unless authorised.
i) Remove License decals or inventory control tags attached to the devices.
j) Disrupt its use by other individuals by connecting to other AICS

networks to perform any illegal or inappropriate act, such as an attempt to gain unauthorised access to other systems on the network.

k) Everyone must honour copyrights and licenses, as well as the legal rights of the software producers and network providers.
l) Use of another person's user account and any access of credentials is prohibited.
m) Anyone who inadvertently accesses an inappropriate site must immediately leave the site and report it to his/her instructor or supervisor.
n) Attempt to log onto the network as a system administrator.
o) Any user identified as a security risk may be denied access to the network.
p) Damage caused by the intentional misuse or vandalism of equipment will be charged to the person who committed the act and will face disciplinary action.
q) Any damage to the school owned devices is the responsibility of the user.

1.10 Improper Use and Content

Users may not use the Intranet/Internet for purposes of harassment, intimidation or bullying of others.

Bullying is the repeated use of a written, verbal or electronic expression, physical act or gesture, or any combination thereof, directed at another student that:

a) causes physical or emotional harm to the student or damage to the student's property;
b) places the student in reasonable fear of physical injury or of damage to property;
c) creates a hostile environment at school for the student;
d) infringes on the rights of the student at school; or,
e) materially and substantially disrupts the education process or the orderly operation of a school.

A hostile environment is a situation in which bullying causes the school environment to be permeated with intimidation, ridicule or insult that is sufficiently severe or pervasive to alter the conditions of the student's education.

Cyber-bullying involves an act of bullying through the use of technology or any electronic communication, including but not limited to electronic mail, internet communications, or instant messages. Cyber-bullying also includes the creation of a web page or blog in which the creator assumes the identity of another person; or, the knowing impersonation of another person as the author of posted content or messages, if the creation or impersonation creates any of the conditions described in the definition of bullying. Cyber-bullying also includes the distribution by electronic means of a communication to more than one person or the posting of material on an electronic medium that may be accessed by one or more persons, if the distribution or posting creates any of the conditions described in the definition of bullying.

AICS shall, in its sole discretion, determine whether such conduct violates this Policy and any other policies of AICS. Users must remember that material distributed through the Internet is public. On the Internet, there is no central authority, so each site is responsible for its own Users. Complaints received

from other sites regarding any of our Users will be fully investigated, and disciplinary action may be taken as a result.

1.11 Social Media

While AICS respects the right of employees, students and families to use social media and networking sites, as well as personal websites and blogs, it is important that any such personal use of these sites does not damage AICS's reputation, its employees, or its students or their families. Student use of social networking sites is prohibited on AICS distributed laptops; for student, these guidelines are intended to be applied for personal computer use outside of school. All users should exercise care in setting appropriate boundaries between their personal and public online behaviour, understanding that what is private in the digital world often has the possibility of becoming public, even without their knowledge or consent.

AICS strongly encourages all employees, students and families to carefully review the privacy settings on any social media and networking sites they use (such as Facebook, Myspace, Twitter, Flickr, LinkedIn, etc.), and exercise care and good judgment when posting content and information on such sites. When using a social media site, an employee may not include current students as "friends," "followers" or any other similar terminology used by various sites. If an employee has a community that extends to persons who are parents, alums, or other members of the AICS community, she/he must exercise good judgment about any content that is shared on the site.

Additionally, employees, students and families should adhere to the following guidelines, which are consistent with AICS's community standards on harassment, student relationships, conduct, professional communication, and confidentiality:

a) Users should not make statements that would violate any of AICS's policies, including its policies concerning discrimination or harassment;
b) Users must uphold AICS's value of respect for the individual and avoid making
c) defamatory or disparaging statements about the School, its employees, its students, or their families;
d) Users may not disclose any confidential information of AICS or confidential information obtained during the course of his/her employment, about any individuals or
e) organisations, including students and/or their families.

AICS has a strong interest in promoting a safe and supportive learning environment, as well as maintaining a positive reputation in the community. If the School believes that an employee's activity on a social networking site, blog, or personal website may violate the School's policies or otherwise may have a detrimental impact on the learning environment, the School may request that the employee or student cease such activity. Depending on the severity of the incident, the employee or student may be subject to disciplinary action. AICS reserves the right to impose discipline, up to dismissal or termination, for any behaviour on or off campus that AICS determines may impair or negatively impact the reputation of the School.

1.12 Theft and Vandalism

Users must acknowledge the use of the intellectual property of others. Users must treat information found electronically in the same way as information found in printed sources. Rules against plagiarism will be enforced. It is the responsibility of each User to comply with the terms and condition for the acquisition and use of software found on the Internet. AICS will not allow the copying or storing of illegally acquired software. In this case, vandalism refers to deliberate attempts to damage the hardware, software, or information residing on Intranet or any other computer system attached through the Internet. Attempts to violate the integrity of private accounts, files or programs; the deliberate infecting of a computer with a "virus", attempts at "hacking" computers using any method, or other such actions shall be a violation of this Policy.

1.13 Chain Letters and Other "Spreading" Schemes

Whether in e-mail or in newsgroups, chain letters, pyramid schemes, forwarding or replying to "contests" or "fast cash" schemes, mass cross-postings, and uninvited mass mailings are forbidden on the Internet and on the Intranet.

1.14 "Netiquette"

Users must abide by accepted rules of network etiquette, including, but not limited to, the following:

a) Do not reveal personal information – your address or telephone number, or those of students or colleagues.
b) Be polite. Do not be abusive in your messages to others. Use appropriate language and do not use vulgarities, or any other inappropriate language.
c) Do not use the Intranet in such a way that would disrupt its use by others.

1.15 Waiver of Warranties; Limitation of Liability

AICS makes no warranties of any kind, whether express or implied, concerning this service.
AICS shall not be held responsible for any damages suffered, including the loss of data resulting from delays, non-deliveries, missed deliveries, service interruptions, or errors and omissions. AICS denies any responsibility for the accuracy or quality of information obtained through this service. All terms and conditions as stated in this Policy are applicable to the use of computer resources at AICS, in addition to internet use.

1.16 Entirety of Agreement

The terms and conditions stated in this Policy, and all other policies of AICS incorporated herein, reflect the entire agreement of the parties with respect to the subject matter stated herein. This Policy supersedes all prior oral or written agreements and understandings of the parties. This Policy shall be governed by and interpreted in accordance with the laws of Australia.

1.17 Preservation of Resources

All resources are limited; computer resources are not an exception. Because space on disk drives and bandwidth across the lines, which connect Intranet both internally and externally, are limited, neither programs nor information may be stored on the system without the permission of the system administrator. Users are not to load software on any school computer. Each User is permitted reasonable space to store e-mail, Web, and personal files, as mandated by system file quotas. AICS reserves the right to require the purging of files in order to regain disk space without warning. Users whose need for the resource is more pressing

will have priority of space.

1.4 Special Note Regarding Borrowed Equipment

Because AICS is a day school, and for the convenience of the user community as a whole, AICS provides digital still cameras, digital video cameras, and other equipment for student use.
Users are responsible for any equipment they may borrow, including accessories, and are expected to employ the equipment in accordance with this Policy. If the equipment should be damaged, or lost while the User has assumed responsibility for it, the User will be accountable for the fair replacement value of the equipment

1.18 Consequences

Any person bound by this policy who intentionally and/or knowingly violates this policy shall be subject to action deemed fit by the Management of Australian Islamic College of Sydney and shall also be liable to pay for the current repair or replacement cost of the damaged software and/or equipment. Any user violating the terms of this document will receive appropriate disciplinary action or the Consequences for Misuses document shared with students upon receiving their computers. Students could lose computer/network privileges, and/or receive detention, suspension or expulsion.

Such action shall not preclude adequate civil and / or criminal remedy as per the Applicable law.

Exceptions to a policy must be approved by the Principal with review by ICT Team. In each case, the requestor must include such items as the need for the exception, the scope and extent of the exception, the safeguards to be implemented to mitigate risks, specific timeframe for the exception, organisation requesting the exception, and the management approval.

The ICT Team or his/her designee may close an account at any time as required. The administration, faculty and staff of AICS may make a request to the ICT team or his/her designee to deny, revoke or suspend specific user accounts based upon violations of this policy.

RESPONSIBILITIES

1. The ICT Manager will be responsible for ensuring that this Policy and the relating procedure, is applied to all AICS.
2. Monitoring of Emails - ICT Service Desk Team will be responsible to monitor the emails and to ensure that email usage must complies with AICS Policy.
3. Monitoring of Internet, ICT Service Desk Team will be responsible to monitor the Internet usage and to ensure that internet usage must complies with AICS Policy.

IMPLEMENTATION

The Acceptable usage policy will be implemented throughout the via:

1. An announcement email will be sent to all AICS Employee from 'IT Communication'.
2. Policy, Procedure and forms will be uploaded on the 'SharePoint", intranet portal.
3. Training sessions shall be conducted to raise the awareness among employees and students.
4. Documentation distribution, e.g. Posters / brochures on Notice Board and in Newsletters

Authors: ICT Team & Tahir Siddique
Written: March 2017
First Revision: August 2020
Second Revision: January 2022
Next Review: January 2023