Technology Acceptable Use and Internet Safety Policy

Introduction and Purpose

The Allegiance STEAM Academy (ASA) community is encouraged to make innovative and creative use of information technologies in support of education and research. Use of the ASA network is a privilege and is intended only for purposes consistent with ASA educational business and curricular objectives. The purpose of this policy is to ensure appropriate, responsible, ethical and legal use of technology within the ASA community. This policy is designed to guide faculty, staff, students and guests in the acceptable use of the ASA network and technology systems. This policy is an extension of ASA Student Handbook Policies and Personnel Policies. Students and employees are responsible for appropriate use of the ASA network. Inappropriate use may result in the cancellation of user privileges, disciplinary and/or legal action. Activities that violate state, local or federal law may be subject to prosecution. All users are bound by future updates.

Definitions

Technology is defined as “the body of tools, machines, materials, techniques, and processes used to produce goods and services and satisfy human needs.” (World Book Online Dictionary) ASA network includes the computers, terminals, printers, networks, and related equipment, as well as data files or documents residing on disk, tape, or other media, which are owned, managed, or maintained by Technology Services and/or staff. Privately owned equipment, such as laptops, PDA and home computers are considered ASA network if attached directly or remotely to the ASA network and/or are used to access the network. A User is any person, whether authorized or not, who makes any use of any ASA network from any location.

ASA Network Use

Use of ASA network is restricted to authorized ASA faculty, staff, students and guests. ASA networks may be used only for their intended authorized purposes. All use of ASA network must be consistent with all contractual obligations of the school, including limitations defined in software and other licensing agreements.

- Users must not permit or assist any unauthorized person to access ASA network.
- Users must not defeat or attempt to defeat any ASA security.
- Users must not access or attempt to access data on ASA networks that they are not authorized to access.
- Users must not make any deliberate, unauthorized changes on the ASA network.
- Users must not intercept or attempt to intercept data communications not intended for that user’s access.
- Users must not conceal their identity when using ASA network and must show identification upon request by an ASA staff member.
- Users must not deny or interfere with or attempt to deny or interfere with service to other ASA network users.

- Users must use their specific login ID and password and are responsible for the security of said accounts and passwords.
- Users must observe intellectual property rights and copyright laws.
- Without specific authorization, users of ASA network must not cause, permit or attempt any destruction or modification of data or equipment.
- Users must allow access to, and are responsible for the backup of their own data.
- Users must not conceal or attempt to conceal violations by another user. Users are expected to report violations of this policy.

No Privacy

The ASA Network is not a private means of communication. All data stored, transmitted, processed, or otherwise accessed on the network may be monitored, filtered or recorded without notice to the user. All ASA network technology is subject to these rules, even if it is privately owned. When using the ASA network, users do not have an expectation of privacy in anything they create, store, delete, send or receive on the ASA network. The use of ASA network shall constitute express consent to being monitored. This consent shall authorize ASA representatives to monitor, without prior notification or consent, all technology resource use including, but not limited to, Internet use, emails, audios or visual material, computer transmissions, stored information and deleted information or files. Any use in support of illegal activities must be reported to the authorities. Illegal Acts State and federal laws make it illegal to intentionally access any computer system or network for the purpose of:

- Devising or executing any scheme or method to defraud or extort;
- Obtaining money, property, or services with false or fraudulent intent, representations, or promises;
- Damaging or intentionally disrupting the network by altering or deleting files, or introducing any programs or data designed to cause damage by spreading to other networks;
- Threatening, bullying, or sexually harassing another individual;
- Promoting a forum for any illegal activity;
- Making terrorist threats;
- Sharing and/or distributing pornography;
- Plagiarism;
- Copyright infringement

Users committing any of these acts may be subject to prosecution.

User Rights

Access to all ASA network resources is to be shared equitably among users. ASA attempts to provide, at all times, a secure environment conducive to learning and free of illegal or malicious acts. The school has taken precautions, which are limited, to restrict access to inappropriate, unethical and/or immoral materials.

However, on a global network it is impossible to control all access. A user may accidentally or on purpose discover inappropriate information.

Acceptable Use
Generally: ASA network can be used in the support of teaching, research, public service, work related and administrative functions that support the missions of the school.

Incidental Use
Incidental use of computing resources at the school must not interfere with assigned job responsibilities and may result in only a nominal cost to the school. Incidental use should not be considered private and personal.

Prohibited Uses
ASA declares unethical and unacceptable behavior as just cause for taking disciplinary action, revoking network privileges, and initiating legal action. The following are examples of unethical and unacceptable behavior. The following list of prohibited behaviors is not exhaustive, and is offered for illustration only.

- Using ASA network for distributing copyrighted materials, illegal, inappropriate, threatening or obscene purposes, or in support of such activities. Illegal activities shall be defined as a violation of local, state, and/or federal laws. Inappropriate use shall be defined as a violation of the intended use of the ASA network and/or purposes and goals. Obscene activities shall be defined as a violation of the generally accepted social standards for use of a publicly owned and operated communication vehicle.
- Using an account other than your own and any attempt to gain unauthorized access to accounts on the network.
- Attempting to obtain access to restricted sites, servers, files, databases, etc. and/or attempting to gain unauthorized access to other systems (e.g. “hacking”).
- Using personal computer equipment to access the ASA network without prior permission.
- Installing personal software or uninstalling software without prior permission.
- Using Internet games and/or IRC (Internet Related Chat) not related to core curriculum and without direct teacher instruction.
- Using the Internet for commercial purposes, financial gain, personal business, product advertisement, or use of religious or political lobbying.
- Attempting vandalism. Vandalism is defined as willful or malicious destruction and any intent to harm or destroy data of another user, another agency or network that is connected to the Internet. Vandalism includes, but is not limited to, the uploading, downloading, or creation of computer viruses. It also includes attempts to gain access to a network that is connected to the Internet.
- Degrading or disrupting network equipment, software, or system performance.
- Wasting finite network resources.

- Invading the privacy of individuals or disclosing confidential information about other individuals unless directly related to your work assignment.
- Posting personal communications without the original author's consent.
- Posting anonymous messages.
- Accessing, downloading, storing or printing files that are profane, obscene or that use language that offends or tends to degrade others.
- Harassing others and using abusive or obscene language on the ASA network. You may not use the ASA network to harass, annoy or otherwise offend other people.
- Using material which may be deemed in violation of school policy or the law.
- Downloading music, video or any other files not directly related to the curriculum.
- Communicating threats of violence.
- Using ASA network for plagiarism. Plagiarism is taking ideas or writing from another person and offering them as your word. Credit must always be given to the person who created the information or ideas.
- Using ASA network for piracy (unauthorized use or reproduction of copyrighted or patented material).
- The capture, display or sharing of images of persons without their expressed consent.