ACS Security Awareness and Acceptable Use Policy

September 21

2016

Written and revised by S. Ahmed

Security Awareness and Acceptable Use Policy

1. Overview

All staff members who have roles which require access to Ayesha Community School (ACS) data, or roles which make it possible to obtain access to ACS data, have a responsibility to protect that data. This document lays out a set of requirements to which all members of Ayesha Community School who may have access to ACS data must adhere to.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of Ayesha Community School. These systems are to be used for business purposes in serving the interests of the School and of our students, clients and customers in the course of normal operations.

All staff are required to sign an Acceptable Use Agreement at the beginning of every academic year or as soon as they join the school.

2. Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at Ayesha Community School. These rules are in place to protect the employees and Ayesha Community School. Inappropriate use exposes Ayesha Community School to risks including virus attacks, compromise of network systems and services, and legal issues.

3. Scope

This policy applies to employees, contractors, consultants, temporary employees, and all other workers at Ayesha Community School, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Ayesha Community School.

4. Policy

4.1 General Use and Ownership

1. While network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of Ayesha Community School. Because of the need to protect the network,

management cannot guarantee the confidentiality of employee's personal information stored on any network device belonging to Ayesha Community School.

2. IT recommends that any information that users consider sensitive or vulnerable be encrypted.
3. Users shall be only authorized to utilize Ayesha Community School information resources systems for business purposes for which they have been authorized. Usage of Ayesha Community School information systems and resources for personal usage or on behalf of a third party (i.e., personal customer, family member etc.) shall be strictly prohibited;
4. Introduction of unauthorized copies of licensed software & hardware (piracy/copyright & patent infringement) to Ayesha Community School information resources and the copying of such material shall be prohibited;
5. Only IT Coordinator/Operations Department Staff/authorized vendor shall be allowed to install authorized software on the user's system. User shall not be given the authority to install software;
6. For security and network maintenance purposes, authorized individuals within Ayesha Community School may monitor equipment, systems and network traffic at any time.
7. Ayesha Community School reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

1. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential. Examples of confidential information include but are not limited to: credit card information, company private, corporate strategies, competitor sensitive, trade secrets, specifications, student lists, customer lists, and research data. Employees should take all necessary steps to prevent unauthorized access to this information.
2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System and user level passwords should be changed at least every 90 days (42 days for Windows login)
3. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 15 minutes or less.
4. Employees should secure their workstations by logging off or lock (control-alt-delete for Windows users) when the host (workstation) will be unattended.
5. Use encryption of information in compliance with Information Technologies' Security Policies.
6. Because information contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops in accordance with the corporate security standards, including personal firewalls.

7. Postings by employees from an Ayesha Community School email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Ayesha Community School,
8. All hosts used by the employee that are connected to the Ayesha Community School Internet/Intranet/Extranet, whether owned by the employee or Ayesha Community School, shall be continually executing approved virus-scanning software with a current virus database.
9. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

5. Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of Ayesha Community School authorized to engage in any activity that is illegal under local, state or international law while utilizing Ayesha Community School-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

5.1 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Ayesha Community School.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Ayesha Community School or the end user does not have an active license is strictly prohibited. The use of any recording device such as, but not limited to, digital cameras, video cameras, and cell phone cameras, within the premises of all Ayesha Community School properties is prohibited.
3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
6. Using an Ayesha Community School computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
8. Making fraudulent offers of products, items, or services originating from any Ayesha Community School account.
9. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
10. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
11. Port scanning or security scanning is expressly prohibited unless prior notification to IT is made.
12. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
13. Circumventing user authentication or security of any host, network or account.
14. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
15. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
16. Providing information about, or lists of, Ayesha Community School employees to parties outside Ayesha Community School.
17. Any activity that violates the Prevent duty e.g. using IT equipment to promote extremism and go against fundamental British values.
18.

6. Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within Ayesha Community School's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Ayesha Community School or connected via Ayesha Community School's network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

7. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

8. Definitions

Spam Unauthorized and/or unsolicited electronic mass mailings.

Appendix A : Disclaimer Notice

The following Disclaimer will be used for emails:

This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error then please notify the sender and delete this message from your system.

Whilst all reasonable care has been taken to avoid the transmission of viruses, it is the responsibility of the recipient to ensure that the onward transmission, opening or use of this message and any attachments will not adversely affect its systems or data.

The contents of this message may contain personal views which are not necessarily the views of Ayesha Community School.