Elmhurst College

Acceptable Use Policy

1. Introduction

Elmhurst College is committed to providing a robust suite of technological resources for use by employees, students, and all members of the College community. Elmhurst College is also committed to managing the risk members of the College community and the College as a whole face from illegal, inappropriate, or otherwise detrimental actions involving technology taken by individuals or groups.

All of Elmhurst College's technology-related systems, including but not limited to workstations, laptops, iPads, tablets, mobile devices, servers, printers, operating systems, storage media, campus-based and cloud-based software licenses, and network accounts of all types are the property of Elmhurst College. These systems are to be used for purposes that serve the interests of the College, including students, faculty, staff, and everyone with whom we interact in the course of normal operations.

Effective information security is a key element of College risk management and is the collective responsibility of the entire Elmhurst College community. Effective information security requires the participation and support of every Elmhurst College student, employee and affiliate who deals with information and/or information systems.

It is the responsibility of every individual using any College technology resource to know and abide by the guidelines articulated in this and all related policies.

2. Purpose

The purpose of this policy is to outline the acceptable use of technology at Elmhurst College. Inappropriate use of technology exposes individuals and the College as a whole to many potential risks including malware attacks, compromise of network systems and services, compromise of sensitive information, and legal issues. These rules are in place to benefit all members of the Elmhurst College community by providing robust access to today's powerful technological tools while managing the risks inherent in their use.

3. Scope

This policy applies to the use of all technologies owned or leased by students, employees, third parties, guests, or Elmhurst College itself that are used to engage with Elmhurst College's educational offerings, conduct Elmhurst College business or otherwise interact with Elmhurst College's networks and systems. All students, employees, contractors, consultants, and guests are bound by this policy.

4. Policy

4.1 General Use and Security

4.1.1 All computing devices, including mobile devices, which connect to the Elmhurst College network must comply with the *Network and System Access and Security Policy*.

4.1.2 System level and user level passwords must comply with the *Password Policy*. Providing access to another individual, either deliberately or through failure to properly secure system access, is prohibited.

4.1.3 Passwords for any Elmhurst College account, computing device, or system may never be shared with any individual, whether on campus or off. Contact the Office of Information Services (OIS) for assistance in creating proper accounts for managing shared information.

4.1.4 All system accounts will be issued and managed by OIS in accordance with its procedures for identity and access management.

4.1.5 All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 15 minutes or less. You must lock the screen or log off when the device is unattended with the exception of public use devices.

4.1.6 All members of the College community are expected to use caution when opening email or other attachments received from unknown senders, which may contain malware.

4.1.7 All members of the College community have responsibility for following all specific policies regarding the use of College technologies for personal reasons. Users may be expected to sign an acceptable use agreement.

4.1.8 For security and network maintenance purposes, authorized individuals from OIS may monitor and manage equipment, systems and network traffic at any time.

4.1.9 Elmhurst College reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Sensitive and Confidential Information

4.2.1 Elmhurst College sensitive or confidential information stored on electronic and computing devices whether owned or leased by Elmhurst College, a student, an employee or a third party, remains the sole property of Elmhurst College. You must ensure that sensitive or confidential information is protected in accordance with the College's *Policy on the Definition, Classification, Storage, and Use of Sensitive Information*.

4.2.2 Everyone has a responsibility to promptly report the theft, loss or unauthorized disclosure of Elmhurst College sensitive or confidential information to an appropriate supervisor.

4.2.3 Employees may use or share Elmhurst College sensitive or confidential information only to the extent that doing so is authorized to fulfill assigned job duties.

4.3 Unacceptable Use

The following activities are, in general, prohibited. Individuals may be exempted from these restrictions during the course of 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 a student, employee, guest, or anyone otherwise acting on the behalf of Elmhurst College authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Elmhurst College-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.

4.3.1 System and Network Activities

The following activities are strictly prohibited:

1. Violations of the rights of any person or organization 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 Elmhurst College.

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 Elmhurst College or the end user does not have an active license.

3. Accessing data, a server or an account for any purpose other than conducting Elmhurst College business, even if an individual has authorized access for Elmhurst College related purposes.

4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, email bombs, etc.).

5. Revealing an account password to others or allowing use of an account by others. This includes family and other household members when work is being done at home.

6. Using an Elmhurst College computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws or College policies.

7. Making fraudulent offers of products, items, or services originating from any Elmhurst College account.

8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data for which an individual is not an intended recipient or logging into a server or account that an individual is not expressly authorized to access. 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.

10. Port scanning or security scanning without prior OIS approval.

11. Executing any form of network monitoring without prior OIS approval.

12. Circumventing user authentication or security of any host, network or account.

13. Introducing honeypots, honeynets, or similar technology on the Elmhurst College network.

14. Interfering with or denying service to any user (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 any network.

16. Providing information about, or lists of, Elmhurst College students or employees to parties outside Elmhurst College without prior authorization.

See the *Network and System Access and Security Policy* for additional details.

4.3.2 Email and Communication Activities

When using Elmhurst College resources to access and use the Internet, users must realize they represent the College. Whenever individuals state an affiliation to Elmhurst College, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the College". Questions may be addressed to the Office of Information Services.

The following activities are strictly prohibited:

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. Posting the same or similar non-business-related messages to large numbers of newsgroups (newsgroup spam).

See the *Email Policy* for additional details.

4.3.3 Blogging and Social Media

Blogging and other social media activity conducted by employees, whether using Elmhurst College's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of Elmhurst College's systems to engage in blogging and social media activity is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate Elmhurst College's policies, is not detrimental to Elmhurst College's best interests, and does not interfere with an individual's regular duties. Blogging and social media activity conducted from Elmhurst College's systems are also subject to monitoring.

The following specific policies apply:

1. Elmhurst College's *Policy on the Definition, Classification, Storage, and Use of Sensitive Information* also applies to blogging or social media activity. As such, individuals are prohibited from revealing any College confidential information or any other material covered by the College's policy when engaged in blogging or social media activities.

2. Individuals shall not engage in any blogging or social media activities that may harm or tarnish the image, reputation and/or goodwill of Elmhurst College and/or any member of the College community. Individuals are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or using social media and may not otherwise engage in any conduct prohibited by Elmhurst College's *Non-Discrimination and Anti-Harassment* policy (found in the Elmhurst College Human Resources Policies).

3. Individuals may not attribute personal statements, opinions or beliefs to Elmhurst College when engaged in blogging or social media activity. If an individual is expressing his or her beliefs and/or opinions in blogs, the individual may not, expressly or implicitly, represent themselves as a representative of Elmhurst College. Individuals assume any and all risk associated with blogging and social media activity.

4. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, Elmhurst College's trademarks, logos and any other Elmhurst College intellectual property may also not be used in connection with any blogging or social media activity.

5. Policy Compliance

5.1 Compliance Measurement

The Office of Information Services (OIS) will verify and promote compliance to this policy through various methods, including but not limited to, reports, internal and external audits, and feedback to individuals and campus departments.

5.2 Exceptions

Any exception to the policy must be approved by the Chief Information Officer in advance.

5.3 Non-Compliance

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

6. Related Standards, Policies and Processes

- *Policy on the Definition, Classification, Storage, and Use of Sensitive Information*
- *Network Access Policy*
- *Password Policy*
- *Email Policy*