ACCEPTABLE USE POLICY

Author: The Executive Team Member with Responsibility for IT

Review date: July 2024

Last Update Status: Updated June 2022

1. Overview

The intention of the IT Team for publishing an Acceptable Use Policy is not to impose restrictions that are contrary to Harlow College's established culture of openness, trust and integrity. The IT Team are committed to protecting Harlow College's employees, students, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

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 Harlow College. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every Harlow College employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2. Purpose

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

3. Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct Harlow College business or interact with internal networks and business systems, whether owned or leased by Harlow College, the employee, or a third party. All employees, students, contractors, consultants, temporary, and other workers at Harlow College and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Harlow College policies and standards, and local laws and regulation. Exceptions to this policy are documented in section 5.2.

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

4. Policy

4.1 General Use and Ownership

4.1.1 Harlow College proprietary information stored on electronic and computing devices whether owned or leased by Harlow College, the employee or a third party, remains the sole property of Harlow College. You must ensure through legal or technical means that proprietary information is protected in accordance with the *Data Protection Standard.*

4.1.2 You have a responsibility to promptly report the theft, loss or unauthorised disclosure of Harlow College proprietary information.

4.1.3 You may access, use or share Harlow College proprietary information only to the extent it is authorised and necessary to fulfill your assigned job duties.

4.1.4 Employees and students are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. If there is any uncertainty, employees and students should consult their supervisor or manager.

4.1.5 For security and network maintenance purposes, authorised individuals within Harlow College may monitor equipment, systems and network traffic at any time, per IT's *Audit Policy*.

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

4.2 Security and Proprietary Information

4.2.1 All mobile and computing devices that connect to the internal network must comply with the *Minimum Access Policy*.

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

4.2.3 All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.

4.2.4 Postings by employees and students from a Harlow College email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Harlow College, unless posting is in the course of business duties.

4.2.5 Employees and students must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware or Phishing links.

4.3 Unacceptable Use

The following activities are, in general, prohibited. Employees and students 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 Harlow College authorised to engage in any activity that is illegal under local, state, federal or international law while utilising Harlow 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, with no exceptions:

a. 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 Harlow College.

b. Contravene any government laws, acts or regulations, including but not limited to GDPR, data protection, computer misuse act, etc.

c. Unauthorised copying of copyrighted material including, but not limited to, digitisation and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Harlow College or the end user does not have an active license is strictly prohibited.

d. Accessing data, a server or an account for any purpose other than conducting Harlow College business, even if you have authorised access, is prohibited.

e. 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.

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

g. 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.

h. Using a Harlow College computing asset to actively engage in procuring or transmitting material that is has offensive, sexual, hostile or discriminatory content.

i. Making fraudulent offers of products, items, or services originating from any Harlow College account.

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

k. 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 authorised 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.

l. Port scanning or security scanning is expressly prohibited unless prior permission from IT is granted.

m. 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.

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

o. Introducing honeypots, honeynets, or similar technology on the Harlow College network.

p. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

q. 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.

r. Providing information about, or lists of, Harlow College employees to parties outside Harlow College.

4.4 Email and Communication Activities

When using company resources to access and use the Internet, users must realise they represent the company. Whenever employees and students state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company". Questions may be addressed to the IT Department.

4.4.1 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).

4.4.2 Any form of harassment via electronic means, whether through language, frequency, or size of messages.

4.4.3 Unauthorised use, or forging, of email header information.

4.4.4 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.

4.4.5 Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

4.4.6 Use of unsolicited email originating from within Harlow College's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Harlow College or connected via Harlow College's network.

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

4.4.8 Blogging and Social Media

a. Blogging by employees and students, whether using Harlow 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 Harlow College's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate Harlow College's policy, is not detrimental to Harlow College's best interests, and does not interfere with an employee's regular work duties. Blogging from Harlow College's systems is also subject to monitoring.

b. Harlow College's Confidential Information policy also applies to blogging. As such, Employees and students are prohibited from revealing any confidential or proprietary information, trade secrets or any other material covered by Harlow College's Confidential Information policy when engaged in blogging.

c. Employees and students shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of Harlow College and/or any of its employees and students. Employees and students are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct that is not in line with Harlow College's Equality & Diversity Policy.

d. Employees and students may also not attribute personal statements, opinions or beliefs to Harlow College when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of Harlow College. Employees and students assume any and all risk associated with blogging.

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

4.4.2 Email Forwarding

Harlow College-provided email accounts should be used by staff to conduct business, i.e. you should use this account to send and receive College-related communications and you must not use personal or other email accounts available through third-parties (e.g. Gmail) instead of your staff email account. Automatic forwarding of your staff email account to such personal and/or third-party email services is not permitted.

The reasons for this include:

a. It is not known where third-party email providers store the data, and exporting personal data outside of the EU without a formal data processing agreement is in breach of the EU directive on the transfer of personal data
b. There are issues surrounding access to work-related emails in relation to freedom of information requests and Harlow College records management policies on the retention of documents.

5. Policy Compliance

5.1 Compliance Measurement

The IT team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the IT team 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. Revision History

Date of Change	Responsible	Summary of Change
June 2014	SANS Policy Team	Updated and converted to new format
13 Feb 2018	Ben Nicholl	Updated, modified for use in Harlow College
14 Jan 2020	David Higgs	Addition of 4.4.2 (Email Forwarding)
26 May 26, 2022	David Houghton	Review and minor updates

TRACKING and REFERENCE INFORMATION
Date Approved: 14 June 2022 (Executive Team)
Review Date: June 2024
Author/Responsibility: Executive Team Member with responsibility for IT
Equality Impact Assessment: n/a
List of related policies, procedures and other documents: Information, Security & Compliance Policy Password Construction Guidelines Password Protection Guidelines Remote Access Guidelines Data Protection Policy Removable Media Guidelines Bring Your Own Device (BYOD) Policy
Complaints: If you wish to submit a complaint about the application of this policy or the procedure of it, please send your request in accordance with the provisions of the Grievance Procedure.
Monitoring: The application of this policy and associated procedure will be monitored by Executive Team Member with responsibility for IT.
Easy reading: To receive this policy/procedure in a different format, please contact HR Services