coast
mountain
college

INF-022G

Internet Guideline

Purpose

The purpose of this guideline is to establish the rules for the use of Coast Mountain College (CMTN) Internet for access to the Internet or the Intranet.

Overview

Internet access and usage at CMTN must be managed as valuable and mission-critical resources.

This guideline is established to:

- create prudent and acceptable practices regarding the use of the Internet
- educate individuals who may use information resources with respect to their responsibilities associated with such use.

Definitions

Internet: A global system interconnecting computers and computer networks. The computers and networks are owned separately by a host of organizations, government agencies, companies, and colleges.

Intranet: A private network for communications and sharing of information that, like the Internet, is based on transmission control protocol/Internet protocol (TCP/IP), but is accessible only to authorized employees within an organization. An organization’s Intranet is usually protected from external access by a firewall.

User: An individual or automated application or process that is authorized to access the resource by the system owner, in accordance with the system owner’s procedures and rules.

World Wide Web (www): A system of Internet hosts that supports documents formatted in hypertext markup language (HTML) that contains links to other documents (hyperlinks) and to audio, video, and graphic images. Individuals can access the web with special applications called browsers, such as Microsoft Internet Explorer.

Scope

This guideline applies equally to all individuals granted access privileges to any CMTN information system or resource with the capacity to access the Internet, the Intranet, or both.

Details

Accessing the Internet

Users are provided access to the Internet to assist them in the performance of their jobs. At any time, at the request of management, Internet access may be revoked.

IT may restrict access to certain Internet sites that reduce network performance or are known or found to be compromised with and by malware.

CMTN will use Internet filters to block high-risk content and deny access to any unwanted material or malware in support of INF-002, *Acceptable Use of Information Systems Policy*.

All software used to access the Internet must be part of the CMTN standard software suite or approved by IT. Such software must incorporate all vendor-provided security patches. Users accessing the Internet through a computer connected to CMTN's network must do so through an approved Internet firewall or other security device.

- All software used to access the Internet shall be configured to use a proxy or other means of managing or controlling.
- Bypassing CMTN's network security, by accessing the Internet directly, is strictly prohibited.

Users are prohibited from using CMTN Internet access for:

- unauthorized access to local and remote computer systems
- software piracy
- illegal activities
- the transmission of threatening, obscene, or harassing materials
- personal solicitations.

Expectation of Privacy

Users should have no expectation of privacy in anything they create, store, send, or receive using CMTN's Internet access.

Users expressly waive any right of privacy in anything they create, store, send, or receive using CMTN's Internet access.

File Downloads and Virus Protection

Users are prohibited from downloading and installing software on their PC without proper authorization from IT. Technical controls may be used to limit the download and installation of software.

Downloaded software may be used only in ways that conform to its licence and copyrights. All files downloaded from the Internet must be scanned for viruses using CMTN-approved virus detection software. If a user suspects a file may be infected, he/she/they must notify IT immediately.

Users are prohibited from using the Internet to deliberately propagate any virus, worm, Trojan horse, trap-door, or other malicious program.

Monitoring of Computer and Internet Usage

All user activity on CMTN IT assets is subject to logging and review.

CMTN has the right to monitor and log all aspects of its systems including, but not limited to monitoring:

- Internet sites visited by users
- chat and newsgroups
- file downloads
- all communications sent and received by users.

Frivolous Use

Computer resources are not unlimited. Network bandwidth and storage capacity have finite limits, and all users connected to the network have a responsibility to conserve these resources.

The user must not deliberately perform acts that waste computer resources or unfairly monopolize resources to the exclusion of others.

Such acts include, but are not limited to:

- spending excessive amounts of time on the Internet
- playing games
- engaging in online chat groups
- uploading or downloading large files
- accessing streaming audio and/or video files
- otherwise creating unnecessary loads on network traffic associated with non-business-related uses of the Internet.

Personal use, beyond incidental use of the Internet, may be done only on break room PCs and only in compliance with this guideline.

Content

CMTN uses software that makes it possible to identify and block access to Internet sites containing sexually explicit material or other material deemed inappropriate in the workplace.

- The display, storing, archiving, or editing of such content on any CMTN PC is prohibited.
- Users are prohibited from attempting to access or accessing inappropriate sites from any CMTN PC.

If a user accidentally connects to a site containing such material, the user must disconnect at once and report the incident immediately to IT.

CMTN departments may not host their own websites or contract for the hosting of websites by a vendor without the permission of IT.

Content on all CMTN-hosted web sites must comply with the INF-002, *Acceptable Use of Information Systems Policy* and INF-004, *Safeguarding Member Information Policy*.

No internal data will be made available to hosted Internet websites without IT approval.

No personal or non-CMTN commercial advertising may be made available via hosted CMTN websites.

Transmissions

All sensitive CMTN material transmitted over the Internet or external network must be encrypted. Electronic files are subject to the same records retention rules that apply to other documents and must be retained in accordance with departmental records retention schedules.

Incidental Use

Incidental personal use of Internet access is restricted to CMTN-approved Users; it does not extend to family members or other acquaintances. Incidental use must not result in direct costs to CMTN and must not interfere with the normal performance of an employee's work duties.

No files or documents may be sent or received that may cause legal liability for, or embarrassment to, CMTN.

Storage of personal files and documents within CMTN's IT should be nominal.

All files and documents, including personal files and documents, are owned by CMTN, may be subject to open records requests, and may be accessed in accordance with this guideline.

Reimbursement

An employee, whose position requires him/her/them to have remote access, will be reimbursed for his/her/their Internet expenses up to a reasonable amount. An expense report will need to be completed and submitted to his/her/their manager for approval.

Related Policies, Guidelines, and Other Resources

- INF-001, *Acceptable Use of Information Systems Policy*
- INF-004, *Safeguarding Member Information Policy*