Understanding Acceptable Computing Access and Use Policies

Overview

University policy establishes restrictions regarding the access and use of University technology resources such as computers, computer systems, networks, services, storage, and email. Students, faculty, and staff are obligated to protect University computing systems from illegal or damaging actions, either knowingly or unknowingly.

Detail

The following are considered improper uses of University-owned computing equipment, networks, services, and resources:

- Using information technology resources for purposes other than research or instructional purposes. Computing resources may not be used for commercial purposes or personal gain. Use of computer services for any commercial purpose, partisan political purpose, or for any unlawful purpose is prohibited.
- Intentionally or recklessly abusing or misusing computing resources so as to cause damage, system interruptions, or harassment to other persons.
- Repeatedly or purposefully engaging in activities which can be reasonably expected to, or do, unreasonably tax computing resources or go beyond their intended or acceptable uses.
- Borrowing, lending, falsifying, or misusing a computer account computing resource, or allowing, or facilitating the unauthorized access to use of University computing resources by a third party.
- Obtaining user IDs and/or password(s) of other persons in order to use University or University-related computing resources, or impersonating another person on a computing resource.
- Using electronic media to harass or threaten other persons, or to display, design, copy, store, draw, print, or publish obscene language or graphics.
- Submitting or causing to be submitted to the University false, misleading, harassing, or deceptive help requests or complaints.
- Using University computing resources to gain or attempt to gain unauthorized access to computing resources either inside or outside of the University.
- Intercepting or attempting to intercept or otherwise monitor any communications not explicitly intended for him or her without authorization.
- Copying, reading, accessing, using, misappropriating, altering, publishing, or destroying computer files, output data, documents or other files of another individual or attempts to do so, without the permission of that individual, project leader, or authorized administrator.
- Making, distributing, and/or using unauthorized duplicates of copyrighted material, including software applications, proprietary data, and information technology resources. This includes sharing of entertainment (e.g., music, movies, video games) files in violation of copyright law.
- Violating the terms and conditions of software license agreements for software distributed by the University of Pittsburgh by giving, lending, selling, or leasing such media or software to others for their own use.
- Interfering with the operation of the University's information technology resources by deliberately attempting to degrade or disrupt resource performance, security, or administrative operation including, but not limited to, intentionally introducing any computer virus or similar disruptive force into any computing resource.
- Using a computer, computer system, computer network, or any other University property for the creation, design, manufacture, preparation, display, or distribution of any written or graphic obscene material is prohibited.
- Willfully, fraudulently and without authorization gaining or attempting to gain access to any computer, computer system, computer network, or to any software, program, documentation, data, or property contained in any computer, computer system or computer network is prohibited, including obtaining the password(s) of other persons in order to use University or University-related information technology resources without proper authorization or impersonating another person or an information technology resource. This includes, borrowing, lending, falsifying, or misusing a computer account or allows, or facilitates the unauthorized access to use of University information technology resources by a third party.

University policy also includes more information such as defining who may have access to technology resources, the ownership of email for employees, how to report violations outlines the disciplinary action which can result from violations. For more information, please refer to University of Pittsburgh Policy 10-02-05 Access to and Use of University Computing Resources.

Sign in to leave feedback

0 reviews

Request Help

Print Article

Related Articles (1)

Getting Started with Zoom
Get started with Zoom, an online and mobile meeting solution that combines real-time chat, content sharing, and video.

Related Services / Offerings (1)

Threat Protection
SECURE COMPUTING The University of Pittsburgh has a robust series of security controls to protect from threats including Enterprise Spam and Virus Filter with Exchange Online Protection and Microsoft Defender for Endpoint.

Attachments (0)

No attachments found.

Pitt IT Administrative Offices

Cathedral of Learning, 7th Floor
4200 Fifth Ave.
Pittsburgh, PA 15260

Follow @UPittIT

Technology Help Desk

Submit a Help Ticket

Chat with an Expert

Call 412-624-HELP (4357)

Search Help Articles

Visit a Drop-In Location

Email helpdesk@pitt.edu

Join Our Team

IT Professional Opportunities
IT Student Employment

Technology Training

Instructor-Led Workshops
On-Demand Training (LinkedIn Learning)