Information Technology Acceptable Use Policy

Introduction

This policy is designed to guide students, faculty, staff, and other authorized users (hereinafter referred to collectively as "users") in the acceptable use of computer and information systems and networks provided by Fairfield University. This policy specifically explains the University's position on the acceptable use of its electronic resources, including electronic mail (email), voicemail, internet access, and computer information systems.

The University reserves the right to limit access to its networks through University owned or other computers, and to remove or limit access to material posted on University owned or other computers. Sending, saving, accessing, or viewing obscene or otherwise inappropriate material on the University's electronic resources is prohibited. Messages stored and/or transmitted by the University's electronic resources, including the computer, voicemail, email, or the telephone system, must not contain content that may reasonably be considered to be obscene or other patently offensive material. Prohibited material does not include material accessed for legitimate research, study, or work purposes, and includes, but is not limited to, sexual comments, jokes or images, racial slurs, gender-specific comments, or any comments, jokes or images that would discriminate against or harass someone on the basis of their race, color, sex, age, national origin or ancestry, disability, or any other category protected by federal, state or local law. Likewise, any use of the internet, email, or any other electronic resource to engage in harassment or discrimination prohibited by University policies is unlawful and strictly prohibited. Violators may be subject to discipline.

University computer and information systems and networks, including all University owned equipment and data that is on them (i.e. electronic resources) are the property of Fairfield University. Notice is hereby given that there are no electronic resources supplied by the University that provide for sending or receiving private or confidential electronic communications. System administrators have access to all mail and will monitor messages and other content processed through University's electronic resources.

Materials available on Fairfield University networks do not necessary reflect the views of, nor are they necessarily attributable to, Fairfield University.

Students, faculty, and staff are advised that the acceptable use standards contained within the particular institutional policies applicable to them (i.e. handbooks) supersede this policy where appropriate, and govern their conduct with respect to the acceptable use of University electronic resources.

Responsibilities

Users are responsible for the content of all text, audio, and/or images that they place or send using the University's electronic resources. The following examples, though not covering every situation, specify

some of the responsibilities that accompany the use of electronic resources at Fairfield University and/or networks to which Fairfield is connected.

1. Users may not attempt to modify the University Information Technology facilities, crash and/or disable systems, or tamper with any software protections or restrictions placed on computer applications or files.
2. All users must obtain authorized computing accounts and may only use their own user names and passwords to access University information Technology systems and electronic resources. Users may not supply false or misleading data nor improperly obtain another's password in order to gain access to computers or network systems, data or information. Users should not attempt to subvert the restrictions associated with their computer accounts.
3. Users are responsible for all use of their computer account(s). They should make appropriate use of the system and network-provided protection features and take precautions against others obtaining access to their information technology resources. Individual password security is the responsibility of each user.
4. Users may not encroach on others' use of computer resources. Such activities would include, but are not limited to, tying up computer resources for excessive game playing or other trivial applications; sending frivolous or excessive messages, including chain letters, junk mail, and other types of broadcast messages, either locally or over the internet; using excessive amounts of storage intentionally introducing any malicious software such as viruses, worms, Trojan Horses, ransomware, or other rogue programs to Fairfield University hardware, software, or networks; attempting to access another user's credentials or computer; physically damaging systems; or running grossly inefficient programs when efficient ones are available.
5. Fairfield University equipment and software may not be used to violate copyright or the terms of any license agreement. No one may inspect, modify, distribute, or copy proprietary data, directories, programs, files, disks or other software without proper authorization.
6. Users must not connect unauthorized devices to the University networks, including wireless networks, without authorization. Unauthorized devices include, but are not limited to, any of the following:
    a. Wireless Access Points (e.g., Apple AirPort Base Stations, Linksys or NetGear Access Points or Gateways, etc.)
    b. Network routers and switches
    c. Devices or computers running network server services such as DHCP, DNS, SMTP, WINS, or acting as a network router
    d. Wired and wireless networked printers
    e. Any devices designed to potentially impede the functionality of other users or computers on University networks
7. Users should exercise their best judgment and due care to prevent the theft of University provided computing devices that have been assigned to them.
8. Users must promptly report the theft, loss, suspected breach of security, or unauthorized disclosure of University data to the Help Desk, or Public Safety if the Help Desk is unavailable.
9. Users must only access, use, or share private or restricted University data to the extent it is has been authorized by data stewards. In cases where that is not clear users should refer to the

helpdesk and handle data as if it were private.

10. Users may not duplicate any licenses, software or related documentation for use either on the University's premises or elsewhere unless the University is expressly authorized to do so by agreement with the licensor.

Information Technology Acceptable Use Policy

Management of Policy

Responsible University Administrator: Chief Information Officer
Created:1/1/1994
Last revised: 7/2022
To be reviewed on or before: As needed