Fairfield
UNIVERSITY

Information Technology Acceptable Use Policy

INTRODUCTION

This policy is designed to guide students, faculty, staff, and other authorized users in the acceptable use of computer and information systems and networks provided by Fairfield University according to the mission of the University. It is meant as an application of the principles of respect and reverence for every person, the development of community and the ideals of liberal education that are at the core of Fairfield's Jesuit Catholic identity.

GUIDING PRINCIPLES

The Fairfield University community is encouraged to make innovative and creative use of information technologies in support of education and research. Access to information representing a multitude of views on current and historical issues should be allowed for the interest, information and enlightenment of the University community. Consistent with other University policies, this policy is intended to respect the rights and obligations of Academic Freedom, and recognizes that the educational mission of the University is served in a variety of ways.

The University recognizes that the purpose of copyright is to protect the rights of the creators of intellectual property and to prevent the unauthorized use or sale of works available in the private sector. Publication, distribution, or broadcast of copyright protected materials without permission is prohibited. Also consistent with other University policies, an individual's right of access to computer materials should not be denied or abridged because of race, creed, color, age, national origin, gender, sexual orientation, or disability.

The University cannot protect individuals against the existence or receipt of material that may be offensive to them. As such, those who make use of electronic communications are warned that they may come across or be recipients of material they find offensive. Those who use email and/or make information about themselves available on the Internet should be forewarned that the University cannot protect them from invasions of privacy and other possible dangers that could result from the individual's distribution of personal information.

In the interests of promoting the free exchange of ideas, Fairfield University does not exercise prior review of electronic documents available on its network and accessible locally or through the internet. Individuals who access materials available on the Fairfield University network should understand that these materials, unless otherwise posted, do not necessarily reflect the views of Fairfield University. Individuals who feel that particular materials posted on the Fairfield University network are inappropriate or otherwise objectionable, may lodge a formal complaint through the Information Technology Services department.

Information Technology Acceptable Use Policy

Fairfield University Information Technology resources are to be used for University-related research, instruction, learning, enrichment, dissemination of scholarly information, and administrative activities. The Information Technology facilities of the University are limited and should be used wisely and carefully with consideration for the needs of others. Information Technology systems offer powerful tools for communication among members of the community and of communities outside the University. When used appropriately, these tools can enhance dialog and communication. When used unlawfully or inappropriately, however, these tools can infringe on the rights of others.

Responsibilities

The following examples, though not covering every situation, specify some of the responsibilities that accompany Information Technology use at Fairfield University and/or networks to which Fairfield is connected.

1. Users may not attempt to modify the University Information Technology facilities or attempt to crash or disable systems. They should not 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. 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. The negligence or naiveté of another user in revealing an account name or password is not considered authorized use. Convenience of file or printer sharing is not sufficient reason for sharing a computer account. 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. University-owned computers, iPads, MiFi devices and the data that is on them are property of Fairfield University and controlled by ITS and should be returned to the hiring manager upon termination/resignation. Any University equipment not returned will be remote disabled and replacement cost will be charged to the departmental budget.
5. 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 harassing messages; 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 (as determined by Information Technology Services policies); 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 acquire another user’s credentials or gain access to their computer; physically damaging systems; or running grossly inefficient programs when efficient ones are available.

6. Users are responsible for making use of software and electronic materials in accordance with copyright and licensing restrictions and applicable University policies. 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.
7. Users must remember that information distributed through the Information Technology facilities is a form of publishing, and some of the same standards apply. For example, anything generated at Fairfield that is available on the Internet through the University's network represents the University and not just an individual. Even with disclaimers, the University is represented by its students, faculty and staff, and appropriate content, language and behavior is warranted.
8. 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
9. Users should use their best judgment such to prevent the theft of the University provided computing devices that have been assigned to them.
10. 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.
11. 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 their direct supervisor and handle data as if it were restricted.
12. Users must protect sensitive printed University data they handle or store with due care including ensuring sensitive information is not left unattended, publicly viewable, in unlocked offices, or on publicly accessible printers.
13. Users must protect electronic sensitive University data they handle, store, or process with due care including ensuring only authorized applications are installed on computer systems used to store, process, or handle sensitive University data. Users must adhere to University policies concerning the safe handling of sensitive data.

ADMINISTRATION

The University encourages all members of its community to use electronic communications in a manner that is respectful to others. While respecting users' confidentiality and privacy, the University reserves the right to examine computer files and monitor electronic activity within the limits of other applicable University policies. The University may exercise this right in order to enforce its policies regarding harassment and the safety of individuals; to prevent the posting of proprietary software or electronic copies of electronic texts or images in disregard of copyright restrictions or contractual obligations; to safeguard the integrity of computers, networks, and data either at the University or elsewhere; and to protect the University against seriously damaging consequences. The University may restrict the use of its computers and network systems for electronic communications when faced with evidence of violation of University policies, or federal, state or local laws. 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 computers.

All users are expected to conduct themselves consistent with these responsibilities and all other applicable University policies. Abuse of computing privileges will subject the user to disciplinary action according to established University procedures. Abuse of networks or computers at other sites through the use of Fairfield University resources will be treated as an abuse of computing privileges at the University. When appropriate, temporary restrictive actions will be taken by system or network administrators pending further disciplinary action. The loss of computing privileges may result.

The University and users recognize that all members of the University community are bound by federal, state and local laws relating to civil rights, harassment, copyright, security and other statutes relating to electronic media. It should be understood that this policy does not preclude enforcement under the laws and regulations of the United States of America nor the State of Connecticut.

This policy may be amended or changed by the University Vice Presidents, and in matters affecting the Academic Division, with the mutual consent of the Academic Council.

Fairfield UNIVERSITY

Information Technology Acceptable Use Policy

REVISION HISTORY:

Date	Author	Version Number	Comment
07/08/2019	Justin Hickey	1.0	Original Version
06/14/2022	Henry L. Foss	1.1	Updated to make current

The official version of this information will only be maintained in an online web format. Any and all printed copies of this material are dated as of the print date. Please make certain to review the material on-line prior to placing reliance on a dated printed version.