Technology Acceptable Use Policy for Employees

Introduction

Technology resources at Franklin Pierce University are primarily intended to support the academic and administrative needs of students, faculty, and staff members at the University. The purpose of this policy is to promote the efficient, ethical, secure, and lawful use of these resources by employees.

All technology resources owned, licensed, leased, or otherwise provided by Franklin Pierce or that are used to access the Franklin Pierce network are subject to this policy. Resources include but are not limited to computers, mobile devices, peripheral devices, storage media, classroom and lab technology, software and enterprise database systems, network and web services, and telecommunications services accessible from any University campus or from another location. Resources may be accessible as cloud or on premise services.

Resources of other organizations accessible from the Franklin Pierce network may have their own policies. When accessing another organization's resources from the Franklin Pierce network, employees are responsible for abiding by this policy and the policies of the other organization.

Rights and Responsibilities

Franklin Pierce makes technology resources available to employees in order to support their job function and as such Franklin Pierce reserves the right to limit, restrict, or extend computing privileges and access at any time. Access to these resources is a privilege granted by the University based upon specific need. All technology and electronic communications using that technology (including but not limited to email, text messages, voicemail, etc.) are and remain the exclusive property of Franklin Pierce, subject to the provisions of Article Twenty-Seven of the Collective Bargaining Agreement between The Rindge Faculty Federation and the University, and are not to be considered the private property of any employee, regardless of whether the content of electronic communication is personal or business related or is password protected or otherwise marked personal and/or confidential. Employees should also not assume that when an electronic message or file is deleted that it cannot be recovered.

Franklin Pierce does not intend to act as a censor of information. It does however reserve the right to inspect files, email, or other communications utilizing the University's technology resources to ensure compliance with its policies and to protect the University's network or other

shared resources from disruption and to take appropriate action without first providing notification. Computers, mobile devices, files, email, or other technology may also be subject to search by law enforcement agencies in accordance with applicable law and when properly requested, subpoenaed, or ordered by a court.

Upon hire, each employee is issued one or more accounts to access Franklin Pierce's network resources as required for his or her position. Access to University resources, including access to the network and email system is intended for the sole use of the employee to whom the accounts are issued. These accounts are not transferable without authorization. Employees are responsible for choosing secure passwords, ensuring confidentiality of login procedures, and adequately protecting information on computers, storage media, printers, copiers, faxes, and printed reports (see Franklin Pierce's Information Security Policy). Access will remain in effect until separation from employment or unless otherwise terminated by Franklin Pierce at its sole discretion.

Conduct Which Violates this Policy

While not an exhaustive list, it is **not acceptable** to:

- Allow someone else to use your username and password (unless it has been specifically set up as a generic account) or to use a username and password assigned to someone else.
- Access information for which specific authorization has not been provided.
- Expose confidential or sensitive information to unauthorized individuals.
- Publish or post Franklin Pierce material on web sites or social media sites without authorization.
- Monitor or tamper with another user's electronic communications or read, copy, change, or delete another user's files or software or reconfigure their University-owned computer without authorization.
- Violate copyright laws and their fair use provisions or applicable University policies through inappropriate use, reproduction, and/or distribution of copyrighted works (the unauthorized distribution of copyrighted material may subject the violator to civil and criminal penalties).
- Violate terms of software licensing agreements. This includes but is not limited to installing University-provided software on personally-owned computers unless explicitly permitted to do so or providing University-licensed software to someone else (violators assume sole liability for any resulting cost or fine).
- Install personally-owned or licensed software not sanctioned by Franklin Pierce and not approved by the IT department on University-owned computers or mobile devices.
- Circumvent data protection and security protocols including anti-virus software.
- Knowingly send virus-infected emails or files to others.
- Intentionally or carelessly perform an act that may interfere with normal operations of computers or the network or that may expose these resources to security risks.
- Connect unauthorized equipment to the Franklin Pierce network including but not limited to personally-owned servers, printers, routers, switches, and wireless access points.

- Intentionally or carelessly damage, deface, or alter University-owned computers or other resources.
- Use Franklin Pierce resources for solicitation or commercial activity such as selling of products or services without authorization.
- Use email or other communications technology to harass, defame, or threaten others in violation of Franklin Pierce's sexual harassment and non-discrimination policies. This includes but is not limited to sending offensive messages that contain sexual implications, racial slurs, or other gender-based comments.
- Install or display material on University-owned computers that may be reasonably construed as abusive, profane, or sexually offensive (Franklin Pierce recognizes however that legitimate academic pursuits may include material that may be perceived as offensive).

Employees are responsible for the security of accounts as well as computers and mobile devices used to access the University's network resources from off-campus. Remote access to webmail and other web services is available to all employees with authorized accounts. Remote access through the University's Virtual Private Network (VPN) and remote desktop services is only granted based upon specific need and with supervisor approval.

Franklin Pierce permits personally-owned computers and mobile devices to connect to the University's network with access to Internet resources only. Technical support from the IT department at Franklin Pierce is limited to network configuration on a best-effort basis for personally-owned technology.

Franklin Pierce also permits reasonable use of the University's technology resources for personal reasons as long as it does not interfere with job responsibilities or network operations and is not excessive.

Privacy and Data Collection

We collect location data directly from your devices automatically when you use our wireless networks. We may collect information associated with your device using wireless triangulation, or similar technologies.

The use of this data will be limited to the following purposes:

- To to enhance the security and performance of FPU's networks and information systems;
- To promote the health and safety of Franklin Pierce University community members;

We will retain your data only for so long as is necessary for the purpose for which it was collected, or as otherwise required or permitted by law.

This data is stored and protected in accordance with the Franklin Pierce University Information Policy.

Compliance

Employees using the University's technology resources act as representatives of Franklin Pierce and as such are obligated to use these resources in a manner that is consistent with the policies and values of the University.

By accessing these resources, employees agree to abide by this policy as well as other relevant Franklin Pierce policies and applicable laws, regulations, and contractual obligations.

Violation of this policy may result in the loss of computing and network privileges and/or other disciplinary action. Any offense which violates local, state, or federal laws or regulations may be referred to the appropriate law enforcement agencies.

Employees should notify their supervisor, IT Department, or Human Resources Department if they become aware of any violation of this policy.

Franklin Pierce reserves the right to make revisions to this policy at any time. The University will post the most up-to-date version on the HR and IT web sites and inform employees of significant changes.