Technology Acceptable Use Policy
For Students

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

In general, acceptable use means respecting the rights of other computer users, the integrity of University's technology resources, and relevant licenses, policies, and laws. Students are expected to use Franklin Pierce's technology resources in a responsible manner.

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

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

Rights and Responsibilities
Access to Franklin Pierce's technology resources is a privilege granted by the University and as such Franklin Pierce reserves the right to limit, restrict, or extend computing privileges and access at any time.

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 technology resources provided by the University either on-campus or in the cloud to ensure compliance with its policies and to protect those resources or other shared resources from disruption. In addition, the University reserves the right to take appropriate action without first providing notification when there is reasonable belief that there has been intentional or inadvertent violation of policies or disruption to services. Computers, mobile devices, files, email, and 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. Students should not assume that when an electronic message or file is deleted that it cannot be recreated or recovered.

Students do not own the accounts provided to them by the University to access network resources, but are granted the privilege of exclusive use. Accounts are not transferable and students are responsible for securing their passwords and adequately protecting information on computers, mobile devices, storage media, and printers.

Conduct Which Violates this Policy

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

- Allow someone else to use the username and password assigned to you or to use a username and password assigned to someone else.
- Access information for which specific authorization has not been provided.
- Monitor or tamper with another user's electronic communications or read, copy, change, or delete another user's files or software or reconfigure their computer without the user's permission.
- Violate copyright laws and their fair use provisions or applicable University policies through inappropriate use, reproduction, and/or distribution of copyrighted works including music, videos, and games. The unauthorized distribution of copyrighted material, including peer-to-peer file sharing, may subject the violator to civil and criminal penalties.
- Violate terms of software licensing agreements including installation of software on a computer for which it is not licensed.
- Install personally-owned or licensed software or utilities not sanctioned by the University on University-owned computers.
- Connect a personally-owned Windows-based computer to the Franklin Pierce network without active and up-to-date anti-virus software.
- 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 University-owned computers or the network or that may expose these resources to security risks.
- Connect unauthorized equipment to the University 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 University 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 the University'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.
- Continue to send unwanted or unsolicited electronic communications to someone else after being explicitly requested to stop.
- Forge or misrepresent your identity in an email, text, or other electronic communications.

- 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).

Franklin Pierce sends official electronic correspondence to ***@live.franklinpierce.edu*** student email accounts. Students are therefore expected to check their Franklin Pierce email accounts on a regular basis. Students who elect to forward their ***@live.franklinpierce.edu*** email to another email account remain responsible for correspondence not received because of a defect in the forwarding mechanism or with the destination account.

Students are also responsible for ensuring that their files are securely stored and backed up. Franklin Pierce is not responsible for the recovery of damaged, deleted, or lost files. To foster safekeeping, students are strongly encouraged to save files on their Microsoft OneDrive as part of their Office 365 subscription provided to them by the University.

The IT department will provide support for network configuration and installation of software, including Microsoft Office and anti-virus software, provided by the University. Best-effort diagnostic support will also be provided for other software or hardware-related issues.

Franklin Pierce permits the use of its network resources for recreational purposes, such as games, videos, and music, and for other non-academic purposes. As network and Internet resources have limited capacity however, Franklin Pierce reserves the right to restrict the use of these resources for non-academic purposes based upon bandwidth constraints, institutional priorities, excessive use, or other University policies.

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 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 Security Policy.

Students may opt-out of this data collection by contacting the Office of Student Affairs.

Compliance

Students using the University's technology resources are obligated to use these resources in a manner that is consistent with the policies and values of the University.

By accessing these resources, students agree to abide by this policy as well as other relevant University 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.

Students should notify Student Affairs or the IT 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 Student Affairs and IT web sites and inform students of significant changes.