Acceptable Use

Purpose

This policy defines and describes Phillips Exeter Academy's commitment to ensure the legal, ethical and appropriate use of technology resources at the Academy, including but not limited to computer equipment, software, networks, email, telephones and voice systems.

The technology resources at the Academy are provided to support the Academy's educational and business operations. Academy technology resources, including the information they contain, are the property of the Academy; use of these resources is a privilege and not a right. Individuals who are provided access to Academy technology resources assume responsibility for their appropriate use; the Academy expects individuals to be careful, honest, responsible and civil and to at all times be in compliance with all Academy policies and applicable state and federal law.

Scope

This policy applies to all users of Phillips Exeter Academy's technology resources. It applies to all software and hardware owned, leased or subscribed to by the Academy. It also applies to all personally-owned equipment that connects to the Academy's network. Any use of Academy technology resources is subject to this policy even if such use occurs during non-work hours or off Academy property. All users are required to comply with this important policy. Failure to do so will result in disciplinary action, up to and including termination of employment.

Privacy Expectations

- The Academy's network, voice and computing resources are the property of the Academy. Users should have no expectation of privacy for their access to and use of Academy technology resources (including the information they contain) whether by Academy-provided or personally-owned equipment. To the extent that you use your personal equipment to access and use Academy technology resources, you do not have a personal privacy right in any matter received, sent, or maintained on these systems. To ensure compliance with this policy, the Academy reserves the right to access, view or monitor any information or communication stored on or transmitted over the network, or on or over equipment that has been used to access the Academy's network, and it may be required by law to allow third parties to do so. Electronic data may become evidence in legal proceedings. Information Technology Services (ITS) will participate as required in any investigation as directed by the General Counsel, Dean of Students, Dean of Faculty or Director of Human Resources.
- The Academy places a high value on privacy and recognizes its critical importance in an academic setting. There are nonetheless circumstances in which, following carefully prescribed processes, the Academy may determine that certain broad concerns outweigh the value of an individual's expectation of privacy and warrant Academy access to relevant ITS systems without the consent of the individual. Those circumstances are discussed on the Information Technology webpage, together with the procedural safeguards established to ensure access is gained only when appropriate.

- The Academy reserves the right to protect systems, software, individuals and contents of the network from potential or actual harm.
- Users should exercise caution when storing, processing and/or transmitting personal and sensitive data on their personal equipment or while using Academy technology resources.

Authorized Use

- An authorized user is any person who has been granted authority by the Academy to access its computing, network and voice systems. Unauthorized use is strictly prohibited.
- By accessing the Academy's network using Academy-owned or personally-owned equipment, you have consented to the Academy's exercise of its authority and rights as set out in this policy with respect to any such equipment, as well as with respect to any information or communication stored or transmitted over such equipment.
- When a user ceases being a member of the Academy, this authorization terminates immediately. If a user is assigned a new position and/or responsibilities, authorization to use technology resources not necessary for their new position will also terminate.
- Incidental use for personal, non-business purposes is acceptable, but must not negatively impact system performance, classes, or Academy business.

Responsible Use

- Individuals who are assigned data and voice network accounts are responsible for how they are used. Individuals may not share or borrow accounts and passwords with others.
- Users may not access the personal or confidential accounts and files of others without a legitimate academic or business need. Users are prohibited from acting in ways that are unethical, illegal, or invade the privacy of others.
- Users must maintain the confidentiality of the Academy's sensitive information and comply with Academy information security and privacy policies and federal and state laws.
- Any communication, internal and external, must clearly identify the sender. Individuals may not send messages anonymously or under another name or identity. Altering electronic communications to hide your identity or impersonate another person is prohibited.
- Users are responsible for both the content and possible effects of their messages on the network. Prohibited activities include, but are not limited to, creating or propagating viruses, materials in any form (text, sounds, images, video) that would have an adverse impact on the Academy's mission and/or legitimate education interests, chain letters, inappropriate messages (including discriminatory or harassing material) and billable services.
- Users must abide by all copyright and other laws governing intellectual property use.
- Users are prohibited from using Academy networks or equipment for the acquisition, storage or distribution of any digital content that they do not have legal right to use, including but not limited to copying and sharing software, images, music and movies.
- Users must adhere to all software license provisions. No software will be installed, copied or used on Academy equipment except as permitted by law and approved by the IT department.

- Users are required to have updated virus protection software on their computers when connecting to the Academy network. Users should use caution when opening email attachments or other internet files that may contain malicious software. Any computer found to be infected with viruses or malware to the extent that it may negatively affect Academy resources will have access to network services revoked until such viruses and/or malware have been removed and updated antivirus software has been installed. If a user knows or suspects that their machine has contracted a virus, the user shall notify ITS immediately.

Prohibited Activities

- Attempts to exploit, test, or probe for security holes or weaknesses on Academy computers or networks
- Attempts to monitor, analyze or tamper with network data packets that are not explicitly addressed to your computer
- Using a network address other than the one assigned by the Academy
- Execution or compilation of programs that have the potential to break or interfere with system security
- Use of the Academy's technology resources or data for commercial purposes without prior authorization
- Connecting any secondary physical network, including but not limited to modems, bridges, routers, wireless access points or other network devices to the Academy network without prior authorization from the Director of ITS
- Use that is inconsistent with the Academy's nonprofit status. The Academy is a nonprofit, tax- exempt organization and is subject to specific federal, state and local laws regarding sources of income, political activities, use of property and similar matters.
- Using Academy technology in any way that suggests Academy endorsement of any political candidate or ballot initiative
- Physical theft, rearrangement or damage to any and all Academy technology equipment, facilities or property
- Undisclosed and unauthorized recording or streaming or taking still photographs of other individuals within the PEA community. Individuals are not permitted to make or attempt to make an audio or video recording or take photos of private, nonpublic conversations and/or meetings on the premises, without the knowledge and consent of all participants subject to such recordings, and, in the case of students, without the consent of the Dean of Students. The use of undisclosed hidden recording devices is prohibited, as is the transmission and/or distribution of any such recordings or pictures
- Accessing the Academy's network or equipment to create, access, download, edit, view, store, send or print materials that are illegal, harassing, intimidating, discriminatory, pornographic or otherwise inconsistent with the Academy's stated rules and policies as defined in *The E Book* and this Employee Handbook
- Use of the Academy's technology resources for any type of illegal activity
- Any personal use of Academy technology resources that interferes with Academy work-related activities

- Using a personal email account to conduct Academy business, sending or forwarding Academy-related business information to personal email accounts, or receiving attachments from personal email accounts
- Using any online storage services that are not provided by the Academy for business-related information (e.g., iCloud, Readdle, Dropbox or Box.net)
- Storing on Academy technology resources any Trade Secrets or Confidential Information that users may have acquired from their former employer or any other person or entity to whom they owe a duty to keep such information in confidence, unless such storage is explicitly authorized by the Academy and/or the third party and in accordance with applicable law.

Security

- Each user is responsible for the security and integrity of information stored on their computer or voice mail system. Computer accounts, passwords, security codes and other types of authorization are assigned to individual users and must not be shared with or used by others. The Academy reserves the right to bypass such passwords and to access, view or monitor its systems and all of their contents. By accessing the Academy's systems, you have consented to the Academy's right to do so.
- Users may not attempt to circumvent or subvert the security provisions of any system.
- Only authorized persons are permitted to install and repair Academy equipment. Users must use the Academy's anti-theft systems, exercise vigilance when equipment is used outside of Academy premises, and return all Academy equipment when their employment at the Academy ends.
- In the event of theft or other loss of Academy equipment or any other suspected security incident, users should immediately notify the Director of ITS. Enforcement and Sanctions
- All members of the community are expected to assist in the enforcement of this policy. Violations of this policy may result in a variety of disciplinary actions, which may include the loss of computer, telephone or network access privileges, or dismissal for employees and requirement to withdraw for students. Some violations may constitute criminal offenses as defined by applicable local, state and federal laws, and the Academy may initiate or assist in the prosecution of any such violations to the full extent of the law.
- Any suspected violation of this policy should be reported immediately to the Director of ITS as well as to the Dean of Students, Dean of Faculty or Director of Human Resources.