

# Acceptable Use Policy

## 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 and voice systems.

The technology resources are provided to support the Academy's educational and business operations. Academy technology resources 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 at all times to be in compliance with all Academy policies and with 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.

## 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 his or her 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 solely 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 permission. 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 with federal and state laws.
- Any communication, internal or external, must clearly identify the sender. Individuals may not send any type of message or represent themselves anonymously or under another name or identity. Altering electronic communications or any electronic presence 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 reflect negatively on the Academy, 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 and software-as-a-service provisions. No software may be installed, copied or used on Academy equipment except as permitted by law.
- 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, which 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 networks 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, he or she must 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*, the *Employment Guidelines* and the *Faculty Handbook*.
- Use of the Academy's technology resources for any type of illegal activity.

## SECURITY

- Each user is responsible for the security and integrity of information stored on his or her 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.

## **PRIVACY EXPECTATIONS**

- The Academy's network, voice and computing resources are the property of the Academy. The Academy will, to the extent possible, respect the privacy of all account holders on the network. However, 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. ITS will participate as required in any investigation as directed by the 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. If there is reasonable evidence to suspect a breach has occurred or if the network is being compromised, the user account will be locked while ITS conducts a technical investigation and reports concerns to the appropriate office.
- 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.

## **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 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 information technology as well as to the dean of students, dean of faculty or director of human resources.

*Updated August 2015*