

I. Purpose

The purpose of this policy is to outline the acceptable use of computing and information technology resources at Deerfield Academy including, but not limited to, computer equipment, software, storage media, networks, and electronic mail. These rules are in place to protect the employee/student and Deerfield Academy.

The technology resources at Deerfield Academy are provided to support the educational and administrative activities of the school and should be used for those purposes. Access to these resources is a privilege and not a right and must be treated with the highest standard of ethics.

II. Scope

This policy applies to all users of Deerfield Academy computing resources. This policy applies to all software and equipment that is owned or leased by Deerfield Academy. It also applies to all personally-owned equipment, including wireless devices that may connect to the Academy's network or information systems.

III. Authorized Use

- a. An authorized user is any person who has been granted authority by Deerfield Academy to access its computing, network and telephone systems and whose usage complies with this Policy. 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 authority and rights as set forth 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.
- b. When a user ceases being a member of the Academy or if such user is assigned a new position and/or responsibilities, use of technology resources for which he or she is not authorized shall also cease.
- c. Incidental personal use must not interfere with the employee's performance or with the Academy's ability to use the resources for professional and academic purposes and must be consistent with Academy standards of ethical and polite conduct.
- d. Except as authorized by the CFO, use of the Deerfield Academy technology resources or data for personal business, political campaigning, or commercial purposes is prohibited. Faculty members and students are provided with email accounts, voice mail accounts and Internet access. Staff members may be provided with email accounts, voice mail accounts and Internet access upon approval of their department head.

IV. Responsible Use

- a. No user may act in ways that are unethical or that invade the privacy of others. All users must recognize and not violate the intellectual property rights of others.
- b. All users must maintain the confidentiality of the Academy's sensitive information and comply with information security policies and guidelines, including, but not limited to this policy, as well as federal, state and, as applicable, international laws and regulations.



- c. Disclosing and/or gossiping about confidential or proprietary information related to Deerfield Academy, or making public remarks that defame or disparage the Academy, its personnel, its students, or its interests (including but not limited to email, voicemail, instant messaging, chat rooms, or websites/pages), or that recklessly disregards or distorts the truth of the matters commented on, is prohibited.
- d. All users must refrain from activities that waste Academy technology resources or prevent others from using them. Users will not access, modify or delete others' files or system settings without express permission. Tampering with or degrading the performance of an Academy computer system, telephone system, or network or to deprive authorized users of access or use of such resources are prohibited.
- e. 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, material in any form (text, sounds, pictures, video) that reflects adversely on the Academy, "chain letters" (which offer incentives to relay them to others), inappropriate messages (including discriminatory or harassing material), and billable services.
- f. Users may not send broadcast email or broadcast voice mail without prior permission from Information Technology Services.
- g. Altering electronic communications to hide your identity or impersonate another person is considered forgery and is prohibited.
- h. Users will abide by all copyright and other laws governing intellectual property use. Users are prohibited from using Academy networks or equipment for the viewing, acquisition, storage, or transmission of any digital content which they do not have a legal right to use, including but not limited to copying and sharing images, music, and videos.
- i. No software may be installed, copied, or used on Academy equipment except as permitted by law. All software license provisions must be strictly adhered to. Administrative users are prohibited from installing non-Academy-provided software on school-owned systems without permission from Information Technology Services.

V. The Internet

- a. There are risks involved in using the Internet. The Academy cannot guarantee that users will not encounter language, images, or references that are objectionable. To protect personal safety and privacy, Internet users should not give out personal information to others on public information systems. As with email, information that a user places on the Internet is similar to sending a postcard rather than a sealed letter. Its contents may be accessed by system administrators on this campus and elsewhere.
- b. Users must be aware that some material on the Internet is copyrighted and subject to copyright law.

VI. Inappropriate Materials

- a. Deerfield Academy prohibits faculty, staff, and students from keeping all forms of adult content (pornography or what some would consider pornography) at school including, but not limited to, videos, electronic files or other electronic materials.



- b. Accessing the Academy's network or equipment to create, access, download, edit, view, store, send or print materials that are illegal, offensive, harassing, intimidating, discriminatory, sexually explicit or graphic, pornographic, obscene, or otherwise inconsistent with the values and general standards for community behavior of the Academy is prohibited. These provisions are not intended to prohibit an authorized user from carrying out his or her assigned educational, employment, or administrative functions.

VII. Network Resources and Security

- a. All users are responsible for the security and integrity of the Academy's information resources. Computer accounts, passwords, security codes, and other types of authorization are assigned to individual users – sharing authorization information is strictly prohibited.
- b. Removing or relocating Academy-owned technology resources requires prior authorization from Information Technology Services.
- c. Users may not attempt to circumvent the security provisions of any system on the Academy network.
- d. Users are required to have updated virus protection software on their computers when connecting to the Deerfield Academy network. Users should use caution when opening email attachments or other Internet files which may contain malicious software received from unknown sources. 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 all viruses/malware have been removed and updated antivirus software has been installed.
- e. Student use of personally-owned wireless printers, modems, wireless access points, hubs, switches, routers and other network devices is prohibited. Faculty members may install personally-owned wireless access points or other network devices in their residences only with prior permission from Information Technology Services. Ad-hoc wireless networks are not allowed on campus as they have a negative impact on DA network performance.
- f. Personal wireless devices used for video streaming (such as roku) and gaming (e.g. Xbox); as well as Android and iOS phones may not be used on GreenDoor (Deerfield's secure network). They are permitted on DAWireless.
- g. Use of wired Ethernet ports is prohibited in all dorms without written approval from ITS.

VIII. Privacy Expectations

- a. Deerfield Academy employees and students should recognize that there is no expectation or guarantee of privacy in anything they store, send, or receive on the Academy's information systems, including networked file shares or personally-owned computers that utilize the Academy's network. Users should not expect that email, voice mail, or other information created or maintained on the systems are private, confidential, or secure.
- b. Users should exercise caution when storing and processing personal and sensitive information not directly related to Academy business.



- c. The Academy reserves the right to access, view, or monitor any information or communication stored on or transmitted over the network, and it may be required by law to allow third parties to do so. Electronic data may become evidence in legal proceedings. Messages or data may also be inadvertently viewed as a result of routine systems maintenance and monitoring. Any individual monitoring, except as required by law or in situations perceived as emergency, must be authorized in advance by the Director of Information Technology or the Director of Information Technology's designees.

IX. Enforcement/Sanctions

- a. Deerfield Academy uses access controls and other security measures to protect the confidentiality, integrity, and availability of the information on its computers and communications systems. The Academy, at its sole discretion, reserves the right to copy and examine any files or information related to unacceptable use and to protect its network and information assets from systems and events that threaten or degrade operations.
- b. Users in violation of this policy are subject to a full range of sanctions including, but not limited to, the loss of computer, telephone, or network access privileges, disciplinary action, and dismissal/termination from the Academy. Some violations may constitute criminal offenses as defined by local, state, and federal laws and Deerfield Academy may initiate or assist in the prosecution of any such violations to the full extent of the law.
- c. All members of the community are expected to assist in the enforcement of this policy and users are required to report any violations to the Director of Information Technology Services.