TECHNOLOGY ACCEPTABLE USE POLICY

PURPOSE

This policy outlines the acceptable use of computing and information technology resources at Deerfield Academy including, but not limited to, computer equipment, software, storage media, wired and wireless networks, email, and the Internet. 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, not a right, and must be treated with the highest standard of ethics.

SCOPE

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

AUTHORIZED USE

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 is governed by 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.

A. Students and Employees are given email and network accounts, and Internet access.

B. When a user ceases being a member of the Academy or transitions to a new position and/or responsibilities, use of technology resources for which they are not authorized shall also cease or be altered.

C. Incidental personal use must not interfere with the employee's or student's performance or with the Academy's ability to use the resources for professional and academic purposes.

D. Except as authorized by the CFO, use of Deerfield Academy technology resources or data for personal business, political campaigning, or a commercial purpose is prohibited.

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. Utilizing the Academy's technical resources in any manner that violates the Academy's *Code of Conduct, Social Media Policy,* or *Anti-Bullying and Harassment Policy* is strictly prohibited.

D. All users must refrain from activities that waste Academy technology resources or prevent others from using them. Users are prohibited from tampering with or degrading the performance of an Academy computer system, telephone system, or network or depriving authorized users of access or use of such resources. Users will not access, modify or delete others' files or system settings without expressed permission.

E. Users are responsible for the content and impact of their email messages. Prohibited activities include, but are not limited to creating or propagating viruses, sending SPAM, sending messages that contain inappropriate content, and activities related to billable services. Users may not send broadcast email or broadcast voice mail without prior permission from Information Technology Services or Communications.

F. To protect personal safety and privacy, users of the Internet and Social Media applications should not post or share another individual's personal information without their expressed consent.

G. Altering electronic communications to hide your identity or impersonate another person without approval is considered forgery and is prohibited.

H. Users will abide by all laws governing intellectual property use. Students and employees are prohibited from using Academy networks or equipment for the viewing, acquisition, storage, or transmission of any digital content that they do not have a legal right to use, including but not limited to copying and sharing images, music, and videos. Users must be aware that some material on the Internet is copyrighted and subject to copyright law.

I. Any software installed or used on Academy equipment must comply with all state and federal laws, and must not degrade the performance of the computer or the Academy network. All software license provisions must be strictly adhered to.

J. Users may not download, intercept, relay, tunnel, proxy, or share by any other means, protected Academy data, including another individual's credentials, using any system or technology that the Academy has not expressly authorized for such purpose.

K. Users may not develop any software or app that contains or shares data belonging to the Academy or members of the Academy community, or is branded in any way that implies it has been developed or endorsed by the Academy, without the expressed permission of the Director of Information Technology Services.

NETWORK RESOURCES, PRIVACY 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 credentials 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 or the Academy network.

D. Users are required to have updated virus protection software on their Academy-owned or personal computer when connecting to the Deerfield Academy network. Any computer found to be infected with viruses or malware will have access to network services revoked until all infections have been remediated.

E. Users should exercise caution when opening email attachments or other Internet files that may contain malicious software received from unknown sources. Users should be particularly alert to phishing or spear-phishing email and should report suspicious email as directed by ITS. Employees should comply with all required cybersecurity training.

F. Student use of personally-owned wireless printers, hubs, switches, routers and other network devices is prohibited. Ad-hoc wireless networks are not allowed on campus as they have a negative impact on network performance.

G. Users must connect personally-owned computers and/or wireless devices to Deerfield's designated guest network(s).

H. Users are prohibited from connecting to the Academy's network or devices using any method or account that has not be authorized for that purpose.

I. Deerfield Academy employees and students should recognize that there is no expectation or guarantee of privacy on the Academy's information systems or networks, or on personally-owned computers or devices 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, or confidential. 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 support.

ENFORCEMENT/SANCTIONS

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.

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.