ACCEPTABLE USE POLICY

Elmsford Union Free School District
Computer Network and Technology
Acceptable Use Policy for Staff

The Elmsford Union Free School District (the "District") provides technical equipment, software, and systems to support the administrative functions and the educational mission of its schools. This Acceptable Use Policy ("AUP") provides mandatory guidelines for appropriate, responsible, ethical, and legal use of technology devices and systems.

No set of guidelines or rules can cover every contingency. Therefore, in addition to complying with the guidelines and requirements set forth in the AUP, every user of the District's Technology is expected to exercise good judgment. Proper use of the District's Technology helps protect its staff, its students, and the District from legal liability and helps to prevent disruption of and/or damage to the Technology. It is imperative that each staff member review and comply with this AUP.

In the event that this document is translated into any other language, the District will default to using the English version of this document. Any and all judgment will be done using the English version of this document.

Ownership and Purpose

All hardware, software, operating systems, storage media and devices, network accounts, Internet access devices, wireless communication devices and other technology at the District's school and/or facilities or provided by the District or it consultants (collectively "Technology") are the property of the District and not that of anyone to whom Technology is provided or assigned. This technology includes but is not limited to computers, laptops, cell phones, personal digital assistances (ex: Palm or Blackberry devices), computer networks, data and storage devices, Internet access, mechanisms, software, firmware, hardware, cameras, scanners, telephones, interactive "whiteboards," and printers. Technology is to be used solely in furtherance of the District's administrative functions and educational mission. Use of the District's Technology is a privilege, not a right. Violation of the guidelines and requirements in this AUP or other inappropriate use may result in the suspension or revocation of the privilege to use the District's Technology and/or other disciplinary action.

All data, including but not limited to records, files, communications (including e-mail, text messages, instant messages, voicemail messages, and all other messages) generated by or on, stored by or on or transmitted through the District's Technology (collectively "Data") are the property of the District. Employees should not have expectation of privacy in Data even if labeled "private," "confidential" or the equivalent. The District reserves the right to access, view, monitor and disclose Data, at any time for any purpose. Data may include records of access to and content in web-based, password-protected accounts accessed via Technology. An employee's use of the District's Technology constitutes his/her consent to this access and disclosure.

The "deletion" of Data may not eliminate it from the District's Technology devices or systems and the District reserves the right to access, retrieve, view, monitor and disclose any "deleted" data.

The District also reserves the right to remove, delete, modify, or otherwise disable access to any materials that infringe copyright or are otherwise illegal, violate this AUP or are determined to be inappropriate under the guidelines and purposes set forth in this AUP.

Further, the District reserves the right to log/record Internet and e-mail use and to monitor file server and other Technology utilization by users or the District Technology and to remove user accounts/access to prevent unauthorized activity or activity that violates this AUP.

Users are responsible for exercising good judgment regarding the reasonableness of personal use. Users shall keep passwords secure and will not share accounts. Users are responsible for the security of their passwords and accounts. Users are responsible for what is done using their account and password.

Because information contained on portable devices is especially vulnerable, special care should be exercised. Portable devices should never be left unattended, and should not be taken off the property unless permission has been granted. Upon returning to the District with the portable device, DO NOT plug the device back into the network without first speaking with someone in the IT department.

Computers, which include laptops & workstations, cannot be connected to any off-campus network (hard-wired or wireless) without permission from the administration and use of VPN software which is provided by the District.

The District is not responsible for storing personal files of Users. Files on individual machines should be backed-up on a regular basis to your network folder.

It is understood that system administrators, and other IT staff, although expected to adhere to this policy, are not subject to the areas that would make it impossible to do their job(s) effectively and efficiently. In many cases they will be exempt from various provisions within the normal course of duties.

Scope

This AUP applies to officials, employees, contractors, consultants, temporary employees, members of the Board of Education, and all other individuals that utilize or access the District's Technology at the District offices, facilities and/or schools or at any other location including but not limited to via remote access on behalf of the District. This

AUP applies to all Technology owned, leased or licensed by the District or otherwise provided for use by the District.

Proper Use and Affirmation Obligations of Users

1. Users are responsible for exercising good judgment concerning the use of technology.
2. If a password(s) is assigned by the District or created by the user to utilize any Technology device, service or system, the user shall not reveal his/her password to anyone.
3. Each individual in whose name an access account is issued is responsible at all times for its proper use and all usage associated with such account.
4. Users must comply with all laws governing Technology including but not limited to intellectual property rights, such as copyright.
5. Users are expected to abide by generally accepted rules of etiquette. This includes being polite and using only appropriate language. Abusive language, vulgarities and swear words are all inappropriate and prohibited.
6. Only District Technology may be connected to the District network or other Technology. If a consultant, vendor, or visitor needs to connect to the District's Technology, he or she must have prior approval from the Head of the Technology Department and will be required to sign a document stating their business.
7. Each User must log off from any account when he/she completes his/her work or leaves his/her workstation or device, even if he/she remains in the same room or physical location as the workstation or device.
8. If a user believes District Technology has been infected, is non-responsive or is experiencing other performance impairments, he/she must notify their Building Help Folder immediately.

Priority for computer use will always be given to those engaged in classroom or curriculum-related activities.

Prohibited Uses

1. Users shall not use Technology to bully others, to harass others, to infiltrate systems or networks and/or to damage software, components of devices, systems, services or networks (by virus or otherwise), whether that of the District or of a third-party.
2. Users shall not use Technology to access, download, transmit or process material that is pornographic, obscene, offensive, sexually explicit or dangerous to the integrity of the District's Technology or devices, systems, services, software, firmware or networks of any other person or entity.
3. Users shall not reveal their password(s) to others or allow use of their account by others. This includes students and family and other household members when work is being done at home.
4. Users shall not send anonymous messages or files.

5. Use of the Technology in a manner that misrepresents the user or impersonates others is prohibited.
6. Users shall not reveal through Technology the home addresses, phone numbers, social security numbers, photographs or any other personal information about a student unless specifically asked to do so by the administration.
7. Users are prohibited from using Technology for political lobbying, commercial activity (including advertising) or conducting private business.
8. Users shall not install software/applications on District Technology, including software/applications that can be downloaded or uploaded from the Internet for free or upon payment of requisite fees. If a user requires software necessary for the performance of his/her District functions, he/she must contact their Building Help Folder, and the request will be reviewed.
9. Users shall not modify software settings or programs unless specifically told to do so by a District level system administrator.
10. Users shall not make unauthorized copies of District software/data.
11. Users shall not download or install files that are protected by copyright, including but not limited to movies, music, and games.
12. Users shall not disable antivirus software or otherwise prevent regular updates to software.
13. Users shall not circumvent or attempt to bypass the security, filter, screening or blocking software of any Technology.
14. Users shall not install or connect personal hardware or firmware devices to District Technology or otherwise use personal hardware or firmware devices in conjunction with District Technology. Only hardware owned by the District may be installed, connected to or otherwise used in conjunction with District Technology.
15. Users shall not access social networking sites or chat rooms through District Technology unless specifically given permission by the Administration.
16. Users shall not use Technology to receive, transmit or make available to others messages that are racist, sexist, abusive or harassing to others.
17. Port scanning or security scanning is expressly prohibited.
18. Using the network for financial or commercial gain is expressly prohibited.
19. Engaging in the tracking, buying, selling, or trading of stocks, options or other commodities for personal use is expressly prohibited.
20. Users shall not plug any device into any network-jack or phone-jack without previous permission from a District level system administrator.

E-Mail

There should be no expectation of privacy in email messages nor files or data created by, stored on or transmitted through the District’s Technology. Messages and files are subject to access and review by District administrators, legal officials, or law enforcement personnel. All users should be aware that email messages may be archived and that old messages may be accessed. In addition to the foregoing policies, the following apply to email:

1. Users are discouraged from using District email for personal communication and are asked to use their best judgment when doing so.
2. Users shall treat email messages as written communication.
3. Users shall not open email attachments unless the email is from a "trusted" source.
4. Users shall not send email containing attachments that are not related to District business.
5. Users shall not use email to:
    a. Send threatening, harassing, discriminatory, racist, sexist or defamatory messages;
    b. Infiltrate computer systems and/or damage software components of a computer or computer system (by virus or otherwise);
    c. Download or transmit obscene, discriminatory or other inappropriate material;
    d. Access material that is dangerous to the integrity of the District network or Technology;
    e. Reveal information about others, including but not limited to students;
    f. Send anonymous messages or files.
6. Users shall not read, delete, copy, or modify, without permission, email messages of others and shall not interfere with the ability of other users to send or receive email messages.
7. Users shall not send email with personal solicitations or information related to items for sale (ex: tickets).

District Responsibilities

The District endeavors to provide technology which it believes is useful and appropriate for District business and the education of its students. *The District can not and does not make any warranty of any kind, expressed or implied, with regard to Technology provided to its staff and assumes no responsibility for the quality, availability, accuracy or viability of such Technology.* The District will not be responsible for any damages suffered by any user, including, but not limited to, loss of data or service interruptions caused by errors, omissions or negligence of any District user, nor for any reason resulting from the use of District Technology in contravention of the rules set forth in this Policy.

Although filtering software is utilized, the District cannot guarantee that using District Technology will not result in access of information which may be upsetting or offensive.

Sanctions

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, losing computer access on a temporary or permanent basis, suffering financial penalties, and facing possible prosecution for violation of local, state, and federal laws.

Acknowledgement of Receipt of Acceptable Use Policy

The undersigned acknowledges that he/she has reviewed this Elmsford Union Free School District Computer Network and Technology Acceptable Use Policy and agrees to utilize Technology (as defined herein) in compliance with this policy.

____ ________________

Signature Date

____

Print Name