

NEFEC Acceptable Use of Computing Resources

Last revised: 4/22/20

Table of Contents

Introduction.....	3
Rights & Responsibilities.....	3
Restrictions.....	4
Data Handling.....	5
Inappropriate Use of NEFEC equipment.....	6
Other Examples of Inappropriate Use of a Workstation	7
Electronic Communication	8
Examples of Inappropriate Uses of Electronic Communication:	8
Security & Privacy Expectations.....	9
Web pages.....	10
Network Infrastructure.....	10
Wireless.....	10
Virtual Private Network (VPN)	10
Workstation Operating Systems (O/Ss), Virtualization, and Maintenance	11
Enforcement and Adherence	11

For questions concerning this policy, please contact the NEFEC Educational Technology
Operations Manager

Introduction

The mission of the North East Florida Educational Consortium is to help member districts cooperatively meet their educational goals and objectives by providing programs and services that individual districts would not be able to provide as effectively or as economically when acting alone. The Educational Technology Services (ETS) computing and network facilities of NEFEC are a vital component of the academic environment. As part of the educational goal, NEFEC acquires and maintains computers, computer systems, and networks in support of its member districts. These computing resources are intended for NEFEC-related purposes including direct and/or indirect support of the institution and services it provides and are to be used in a responsible, efficient, ethical, and legal manner.

This policy is designed to ensure the safety and privacy of the information that NEFEC is entrusted to maintain. This policy has been established for all NEFEC employees (also referred to as “users” throughout this document) and to all users of the resources provided, whether on NEFEC premises or from a remote location. Additional policies may govern specific computers, computer systems, or networks provided by affiliated entities. This policy may be modified as deemed appropriate by NEFEC. *No resource access will be given to individuals until this Acceptable Use of Computing Resources policy is accepted and signed. Acceptance of this policy is automatically renewed when a user logs into a NEFEC workstation, usually by clicking “OK” to the Acceptable Use Policy brief upon login. This policy will be reviewed annually and updated as needed. Thus, it is highly recommended that users review this policy annually. Refusal to sign this policy will result in the denial or revocation of network access privileges.*

Rights & Responsibilities

The use of NEFEC-owned computing resources such as desktops or laptops, the NEFEC network, or the Internet access provided by NEFEC is a privilege. The rights of academic freedom and freedom of expression apply to all who use NEFEC computing resources. So too, however, do the responsibilities and limitations associated with those rights. NEFEC supports a freedom of expression atmosphere, but the use of NEFEC computing resources, like the use of other State or Federal education-provided resources and activities, is subject to the requirements of legal and ethical behavior. Thus, legitimate use of a computer, computer system, or network does not extend to whatever is technically possible.

The Internet offers access to a wealth of material that is personally, professionally, and culturally enriching to individuals of all ages. Because creation of Internet sites is not monitored, it is possible that individuals might access information they personally find offensive or disturbing. All efforts are made at NEFEC to ensure access to safe, legal, and morally educational websites by providing filters, firewalls, and other security devices that are maintained by NEFEC Operations staff.

Users of NEFEC resources are responsible for making sure that computing devices that leave the NEFEC property in their possession are protected and secured, to the best of their ability, from theft or unauthorized access/use. This includes **any** user other than the authorized employee. Employees are expected to secure by encryption any data that is moved or copied from a NEFEC workstation, server/service, or application via removable media (ex: USB drive, CD, etc) or transferred to any other storage location. In addition, NEFEC Operations staff will take all reasonable measures to further protect and secure such sensitive and protected information by using software and/or hardware to monitor, identify, protect, secure, and block the unauthorized disclosure of such data as also defined in the NEFEC Data Governance Policy (hard copy available upon request).

Users of NEFEC computing devices are responsible for ascertaining authorizations necessary before logging on to any NEFEC resource. Users are responsible for any activity originating from their accounts which they can reasonably be expected to control. Because of this, accounts and passwords may not, under any circumstances, be used by persons other than those to whom they have been assigned by the account administrator. In cases when unauthorized use of accounts or resources is detected or suspected by the account owner, they should change their password and report the incident to the NEFEC IT Staff immediately.

Users of NEFEC resources must comply with federal and state laws, Putnam School Board Policy, NEFEC internal policies and procedures, and the terms of applicable contracts, including software licenses. Examples of applicable laws, rules, and policies include the laws of libel, privacy, copyright, trademark, obscenity and child pornography; the Florida Computer Crimes Act (FCCA); the Children's Internet Protection Act (CIPA); the Electronic Communications Privacy Act; Health Insurance Portability and Accountability Act (HIPAA); Family Educational Rights and Privacy Act (FERPA); Children's Online Privacy and Protection Act (COPPA); and the Computer Fraud and Abuse Act (CFAA). Users who engage in electronic communications with persons in other states or countries or on other systems or networks may also be subject to the laws of those jurisdictions and the rules and policies of those other systems and networks.

Upon completion of user employment, all NEFEC-owned computing-related equipment and related peripherals/accessories that were assigned to said user must be promptly returned to NEFEC Operations or the user's immediate supervisor for later delivery to NEFEC Operations, before the user's final day of employment. Equipment is expected to be in good working order when returned, with the expectation of normal wear and tear.

Restrictions

In order to best serve our districts, NEFEC reserves the right to limit resources to users. This

includes regularly scheduled maintenance and specific times when NEFEC Operations feels user activity may interfere with the efficient operation of the network system as a whole.

Policies set forth will apply to all NEFEC equipment. NEFEC will provide managed devices (e.g. computers, tablets, etc.) to employees as needed, and employees will be given user-level access to their equipment, and any additional authorizations will be granted as needed based on the NEFEC subscribed concept of Least User Privilege/Access (LUP/A). Other elevation of access may be provided by default through another NEFEC subscribed concept of Role-Based Access. If assistance is needed with installing a new program or with a user needing more privileges, a request can be submitted to the NEFEC IT HelpDesk, where it will be reviewed by NEFEC Operations. Most access requests will be forwarded to the appropriate NEFEC manager for approval in the form of a change management ticket. Application installation requests will be granted or denied based on several factors including, but not limited to, appropriateness for work, job requirements, network interruption potential, configuration conflicts, and/or any security threat the application may pose that could endanger NEFEC computing systems. Denied application requests can be appealed through the Operation Manager, who will review the request and may take it to the ETS Self-Directed Team for further review. All software installed on employee workstations must be properly licensed for legal compliance. Personally-owned software installation requests will be reviewed and approved on a case-by-case basis by the Self-Directed Team. Any software or application discovered on an employee computer that is found to not be licensed properly or does not meet the authorization factors mentioned above will be immediately uninstalled and/or removed with or without notice.

Employees must use NEFEC provided devices as their primary work platforms and may not use personally-owned devices for activities outside of basic email and other provided web-based services. I.e. if an employee is using a personally-owned device for more than 10% of the work time, instead of the NEFEC provided and secured device, then it is a violation of this policy.

Data Handling

Outside of email, no other NEFEC or work-related data may be transferred to, downloaded to, or stored on a personally-owned device (e.g. any computer not managed by NEFEC Operations). Work-related data may not be stored on any cloud platform outside of those approved and managed by NEFEC Operations, under a nefec.org account. Approved cloud storage options can be found [here](#) (if viewing the digital version of this policy). Personally-owned devices that are used to access NEFEC email or other services must be protected by a password to access the device and fully encrypted.

The Operations department will develop procedures to push out all updates and settings to prevent

users from having to individually make changes on their machines to be in compliance with NEFEC policies and state/federal auditor recommendations and criticisms.

Personal laptops and other mobile devices brought on to the NEFEC campus must adhere to these policies and will not be allowed access to the NEFEC secure domain/network. All personal devices are treated as insecure and may only access NEFEC's Guest Wireless network. At no time may a personal device be physically plugged into NEFEC's wired network.

Employees are prohibited from attempting to format or otherwise destroy any type of data stored in NEFEC-owned devices. This includes the destruction, removal, or replacement of storage devices, or making said data unreadable through methods such as unmanaged encryption. Upon employee exit, employees may not delete or purge any NEFEC business data/information from any data location (e.g. profiles, home folders, cloud storage, etc.).

Inappropriate Use of NEFEC equipment

Users must not use computing resources to gain unauthorized access to remote computers or to impair or damage the operations of NEFEC computers, networks, or peripherals. This includes blocking communication lines, intercepting or sniffing communications, and running, installing, or sharing virus or malware programs. Users may not attempt to circumvent the security set in place by NEFEC Operations on the user's NEFEC-assigned computing resource(s) (e.g. Workstation) or any other NEFEC-owned equipment. This includes, but is not limited to, resetting or changing Administrative or System passwords; elevating their account permissions; creating new, unauthorized accounts; or using malicious software to steal or collect administrative account credentials. Deliberate attempts to circumvent data protection or other NEFEC security measures stated above will be taken seriously and will result in the immediate loss of network resource privileges. Actions taken to circumvent NEFEC security measures may be viewed as criminal activity under applicable state and federal law. Incidents will prompt a meeting between the employee, the employee's manager, and NEFEC Operations staff, where the intent/abuse will be discussed, documented, then stored with the employee's permanent record, and then appropriate disciplinary action taken.

At no time is it permitted for an individual to try to "unfilter" his or her computer by any means (e.g. proxies, tunnels, etc.). If material is needed that is blocked by NEFEC filters and security applications, an official request should be made in the form of an IT Helpdesk ticket. If the Operations Team cannot determine the appropriate action, the request will be forwarded onto the ETS Self-Directed Team who will discuss the importance of the material and either grant or deny the request.

Vandalism of NEFEC equipment or resources will result in immediate loss of privileges and is subject to Putnam School Board Policy regarding violation of local, state, and/or federal laws. Vandalism is defined as any malicious attempt to harm or destroy hardware, software, and/or data. This includes the creation of or the uploading of computer viruses onto the Internet or host site. Deliberate attempts to destroy, degrade, or disrupt a NEFEC system's operation and/or performance will be viewed as criminal activity under applicable state and federal law.

Other Examples of Inappropriate Use of a Workstation

- Using the Internet for any illegal purpose (e.g. “hacking,” sharing copyrighted content, etc.)
- Violating staff's rights to privacy including the unauthorized disclosure, use, and dissemination of personal information
- Using profanity, obscenity, or other inappropriate language
- Sending or forwarding pornographic text and/or graphics
- Sending or receiving copyrighted materials or protected trade secrets for distribution without explicit permission
- Reporting or sharing personal communications without the author's prior consent
- Use for commercial activities, product advertisement, or political lobbying
- Using any email account, other than your own, without the owner's knowledge or preauthorization
- Printing copyrighted material without permission
- Disrupting or interfering with other computers or network users, services, or equipment
- Representing oneself as another person (Identity Theft)
- Using computing resources for commercial or personal financial gain
- Storing personal, or not work-related, files
- Removal or destruction of Property Tag (if present)
- Physical modifications to a workstation, such as stickers, covers/skins, or anything else that causes irreparable damage, without prior consent/approval from the IT department

Occasional personal use of computing resources for purposes other than work is permitted when it does not consume a significant amount of resources, does not interfere with the performance of the user's job or other responsibilities, and is otherwise in compliance with this policy. Further limits may be imposed upon personal use in accordance with normal supervisory procedures concerning the use of NEFEC resources.

The NEFEC IT Helpdesk and/or Operations department is responsible for servicing, maintaining, and disposing of all computing-related assets. All IT-related purchases (hardware and/or software) must be funneled through Operations for approval to ensure compatibility, policy compliance, and proper specifications. Users are strictly prohibited from utilizing a third-party service for purchasing, upgrading, and/or repair/troubleshooting (e.g. Apple store, Staples, BestBuy

[GeekSquad], etc.) of NEFEC-owned technology resources. Users are also strictly prohibited from attempting to physically service or modify in any way (e.g. add/remove/change components) a NEFEC-owned technology resource.

Lost or stolen devices must be immediately reported to NEFEC Operations in the form of an IT Helpdesk ticket or phone call. The longer a device goes unreported, the less likely the chances of recovery, and the more likely data existing on the device or accessible by the device's user will be compromised.

Electronic Communication

For purposes of this document, electronic communication includes email, web pages, point-to-point messages (IM/chat/txt), postings to newsgroups or listservs, and any electronic messaging involving computers and computer networks.

Retention periods must be followed for all electronic communication as required by the Florida Public Records Law.

Examples of Inappropriate Uses of Electronic Communication:

While not an exhaustive list, the following uses of electronic communication are considered inappropriate and unacceptable and are prohibited:

- Initiation or re-transmission of chain mail, hate-mail, or any threatening or abusive email sent to individuals or organizations that violates NEFEC's Code of Conduct
- Virus hoaxes
- Spamming or email bombing attacks - Intentional email transmissions that disrupt normal email service
- Unsolicited email that is not related to business and is sent without a reasonable expectation that the recipient would welcome receiving it (Junk Mail)
- False identification - Any actions that defraud another or misrepresent or fail to accurately identify the sender
- Forwarding religious and/or political email
- Using NEFEC resources for personal gain
- Discussing confidential or sensitive information through insecure electronic communication (e.g. standard, unencrypted email)
- Disrespectful, obscene, or inflammatory language; ethnic or racial slurs; and bullying
- Revealing, publicizing, using, or reproducing confidential or proprietary information
- Transmitting inappropriate pictures, videos, or other types of electronic media or software

Email is subject to the Florida Public Records Law to the same extent as it would be on paper. Email may not be used to transfer any sensitive or protected information. This includes information in the body of the email or inside attachments, unless the attachment is encrypted with at least AES-level encryption. It is highly recommended to share files via an approved cloud storage provider instead of emailing attachments.

Security & Privacy Expectations

NEFEC is subject to Florida Statutes regarding public information access. As such, all electronic messages and documents are a matter of public record, and employees should have no expectation of privacy as it pertains to electronic communications, documents, compute resource usage, etc.

NEFEC employs various measures to protect the security of its computing resources. Users should be aware that security and confidentiality cannot be guaranteed. Therefore, all users should practice “safe computing” practices, guard and protect their passwords, and never give out private information over the Internet.

While NEFEC does not actively monitor individual usage of its computing resources, the normal operation and maintenance of computing resources requires the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns, and other such activities that are necessary to provide quality service and policy/law abidance. NEFEC Operations may also specifically monitor the activity and accounts of individual users of computing resources, including individual login sessions and the content of individual communications, without notice, when any of the following apply:


- An account appears to be engaged in unusual or excessive activity
- The user has voluntarily made content accessible to the public, as by posting to Usenet or a web page
- It reasonably appears necessary to do so to protect the integrity, security, or functionality of NEFEC and/or its member districts or to protect NEFEC from liability
- There is reasonable cause to believe that the user has violated or is violating this policy

Any such monitoring of communications, other than what is made accessible by the user, required by law, or necessary to respond to perceived emergency situations, must be authorized in advance by an appropriate member of NEFEC Administration. NEFEC, in its discretion, may disclose the results of any such general or individual monitoring, including the contents and records of individual communications, to appropriate law enforcement agencies and may use those results in appropriate disciplinary proceedings against the user.

It is recommended that employees *never* use or save personal (e.g. non-work related) credentials

on any NEFEC-owned device. Employee's accept full responsibility for personal credentials compromised this way, and NEFEC holds no liability.

Web Pages and Social Media

Official NEFEC web pages and social media sites that represent the consortium are intended for the official educational functions of the organization. Users may not create any internet website or social media sites, under any service, that represents the consortium without official approval from NEFEC Administration. Please see the  NEFEC Social Media Policy for more information.

Network and Server Infrastructure


Users must not attempt to implement their own network and/or server infrastructure. This includes, but is not limited to, physical or virtual network devices such as hubs, switches, routers, firewalls, and/or wireless access points that connect to NEFEC networks in any way. Users may not setup or run any unauthorized servers and services that host NEFEC data or represent NEFEC in any way, no matter where they are located (e.g. on the NEFEC campus, at home, or in the cloud). Examples of such servers and services would be websites, DHCP, DNS, etc. Users are strictly forbidden to hardwire any device to the network that is not owned and managed by NEFEC. Users may not setup and connect anything that is considered an Internet of Things (IoT) device to any NEFEC access point or network. If such a device is needed for work purposes, NEFEC Operations must approve the device's use.

Wireless

Wireless is shared media and can be more easily intercepted by a third party. Wireless users are encouraged to be cautious when connecting to and using access points outside of the NEFEC campus.

No unauthorized Wireless Access Points (WAPs) or Hotspots (e.g. via a cell phone) may be used while on NEFEC property, as they can cause a denial of service to legitimate wireless users, present a method of circumvention, or compromise the security of the NEFEC network. The purchase of travel WAPs for use outside of the NEFEC property, or well away from NEFEC buildings, must be authorized by that department's manager.

Virtual Private Network (VPN)

A NEFEC-hosted remote access VPN must be authorized by the  ETS Self-Directed Team and then granted by Operations. NEFEC's enterprise VPN software may never be used on a personal (non-

NEFEC owned) laptop or other mobile device that is used to connect to and access the NEFEC network, or on a NEFEC computing resource that is known or thought to be compromised (e.g. infected or security otherwise compromised). Private or personally-owned VPN software of any type is not permitted on NEFEC-owned devices.

Workstation Operating Systems (O/Ss), Virtualization, and Maintenance

NEFEC supported operating systems and versions of said operating systems are determined by NEFEC Operations. When a version becomes obsolete, it will be required to be upgraded. No other operating systems are permitted on NEFEC-owned employee workstations. Only a single operating system is to be installed per workstation. “Dual-booting” the aforementioned operating systems or any other operating system is not permitted.

NEFEC-owned employee workstations may not be setup as a virtual host for virtual machines/computers. They can be virtual machines themselves, but they cannot run any type of virtual computer on top of the installed operating system. Exceptions to this rule can be made on a case-by-case basis for NEFEC IT staff only, as required to perform a job function.

Workstations require regular hands-on maintenance by IT staff. Upon request, any mobile or off-site workstations must be brought back to the IT department in a timely manner for manual maintenance such as updates, licensing, security checks, etc. Please expect routine requests throughout the year.

It is highly recommended that all mobile laptops are brought into NEFEC and logged into at least once a month for syncing. This does not require intervention from IT unless there's a problem.

Enforcement and Adherence

Users who violate this policy are subject to Putnam School Board Policy. Failure to adhere to this agreement may result in suspension or revocation of the offender's privilege of access to NEFEC resources, and other disciplinary action up to and including the termination of the employee.

NEFEC Acceptable Use Policy

I acknowledge that I have received, read, and understand that I must adhere to the Acceptable Use of Computing Resources policy as a condition of employment and receiving access to NEFEC, and in some cases, member district data and resources.

I also understand that the willful violation or disregard of any of these guidelines and policies may result in my loss of access privileges and disciplinary action, up to and including the termination of my employment, and/or any other appropriate legal action.

I will make every reasonable effort to protect NEFEC data and resources by following and abiding by this policy, using industry standard information security practices, protecting resources allocated and granted to me, and making good decisions when handling and transmitting sensitive data.

This policy has been reviewed by me on _____.
(date)

Full Name (Print Please) _____

Signature: _____