

# **OHIO VALLEY EDUCATIONAL COOPERATIVE**

## **TECHNOLOGY ACCEPTABLE USE POLICY**

**03.13211**

Referenced by OVEC Policy Manual and OVEC Employee Handbook

**Version 1.2.6**  
**5/17/2006**

Subject headings:

- Introductory paragraph
- Definition of Technology Resources
- Expectations and Standards
- Responsibility and Compliance
- Pornography, Sexual Harassment, and Other Objectionable Material
- Email
- User Accounts: Local Area Network and Email
- Data Storage and Protecting Against Data Loss
- Addition of Workstations and Workstation-Shared Printers
- Addition of Network Printers and Hardware
- Workstation Maintenance
- Copyright and Software Licensing
- Prohibited Software
- Security Software

### **03.13211 OVEC Technology Acceptable Use Policy**

Employees are expected to use OVEC electronic media, networks and other information technology resources appropriately and in compliance with this policy and applicable state and federal legal requirements. The purposes of this policy are to:

1. Educate;
2. Provide protection against privacy violations and misuse of OVEC resources, inappropriate or destructive behaviors that occur as a result of employee access to electronic information resources; and
3. Ensure that the technology resources of OVEC are dedicated to improving service and raising productivity.

Appropriate and inappropriate use of technology resources shall be consistent with the criteria that guide decisions about other OVEC assets.

#### ***Definition of Technology Resources***

The policy applies to computer hardware (workstations, laptop computers, servers, PDAs, etc.) and peripherals (printers, scanners, external hard drives, etc.); the telephone/voice mail system and fax machine(s); alarm system; software (applications, services, operating systems, etc.); network appliances such as routers and switches; network services such as email and internet access; local area network access; storage devices; and databases, files, and other repositories of information in electronic form that are the property of OVEC. In addition, this policy applies to both onsite and remote access.

#### ***Expectations and Standards***

*The knowledge to make use of technology resources necessary for the execution of job duties is the responsibility of the employee.* This includes knowledge of basic computer operation as well as remembering passwords and preventing others from knowing those passwords except when deemed necessary to the execution of job responsibilities.

OVEC has made and continues to make investments in technology with the following expectations concerning its use by employees:

1. Appropriate technology use increases productivity; generally, work products can be produced and services can be delivered with greater accuracy, in less time, and at less cost.
2. Decision-makers will have rapid access to more complete and accurate information.
3. Communication among staff, between the staff and their customers, and with the public will improve.
4. OVEC services and information will be more widely and equitably accessible.

In this spirit, OVEC technology resources may not be used for private business or personal gain. The following misuse of OVEC technology resources is strictly prohibited:

- For private business purposes;
- For a non-work related club or organization;
- To obtain money, property or services for personal or private sector use;
- For political or religious purposes; and
- For the playing of games or participation in contests.

By law, the CTO, CEO, or an individual authorized by either may examine files, transaction logs, email correspondence, or other information about an individual's use of technology resources. Electronic information stored on OVEC technology equipment is considered OVEC property. Further, employees should be aware that email logs, the content of email, logs or internet access, and the content of internet sessions may be subject to inspection under the Open Records Laws (KRS 61.870-61.884 and KRS 171.410-171.720).

If an employee is unavailable, his or her supervisor may be provided with access to the employee's workstation, files, and email account without the employee's permission or prior notice.

### ***Responsibility and Compliance***

Members of the OVEC leadership team (CEO, Program Directors and Coordinators) are responsible for orienting employees within their organizational authority to the provisions of this policy, monitoring compliance, and taking appropriate disciplinary action when inappropriate use occurs.

Employees are responsible for their own actions and the actions of those they knowingly permit to use assigned resources and passwords. Passwords are to be chosen and protected carefully. Employees are encouraged to secure a workstation temporarily by setting a screensaver password.

By law, OVEC itself will not be held responsible for a user's abuse of any OVEC technology system, including email; ultimate legal responsibility rests upon the user. The tier of consequences for violations of the OVEC Technology Acceptable Use Policy is as follows:

1. Loss of network/technology access
2. Disciplinary action per OVEC Policy, up to and including termination
3. Legal action

Employees may not use a password or key code, access a file, or retrieve any stored communication unless they have been given authorization to do so. Employees cannot expect confidentiality or privacy of information exchanged via email. The CTO, CEO, or personnel authorized by either may monitor the use of OVEC technology resources at their discretion. Employees may be required to surrender their password on demand to their supervisor, the CEO, or the CTO.

Security is every user's responsibility. If a user identifies a security problem within the OVEC network, that user is obligated to report the suspected problem to the Chief Technology Officer. Do not demonstrate the problem to other users.

### ***Pornography, Sexual Harassment, and Other Objectionable Material***

Employees shall not use OVEC technology resources to copy, create, send, store, display or distribute pornography and other objectionable materials. This includes, but is not limited to:

- Placing such materials on or retrieving them from a file server, hard drive, or other storage media;
- Sending or receiving pornography and objectionable materials through the network; and
- Using OVEC resources and/or network access to download from or post such materials to personally owned devices.

Objectionable materials include information from hate groups and materials posted to harass or threaten. In addition, pornography viewed by others inadvertently may constitute grounds for sexual harassment.

### ***Email***

Email communications taking place either through the OVEC email server or through another email server to which a user connects remotely shall adhere to the following criteria:

- No sexually explicit or obscene material as described above
- No religious material
- No biased political material
- Do not access another's email without permission except when necessary for the administration of the network email system
- No chain letters and other non-work related correspondence
- No email with attached files that are larger than reasonable – for example, as of 5/3/06 files larger than 12mb are prohibited by the email server software

### ***User Accounts: Local Area Network, Web Services and Email***

Only the Chief Technology Officer (CTO) may create, edit, or delete LAN login, OVEC internet server, or email accounts. The CTO must be notified immediately upon any changes in the personnel status of any employee with an existing network account; such accounts may be retained for a reasonable period after a resignation or termination if necessary (with the consent of his/her supervisor, the CTO, or the CEO). Users are responsible for the security of their user accounts. If passwords are distributed to others besides supervisors or the CTO, the user is responsible for the actions of those to whom access is given. If the user leaves the workstation unattended with applications open, the user is responsible for resulting inappropriate use or security violations.

By request, a user may be given a secure (NTFS-level) subdirectory within the **\\Storage** server on the network, subject to the approval of his or her supervisor. Only the CEO and the CTO may be granted Administrator rights to the OVEC domain.

### ***Data Storage and Protecting Against Data Loss***

It is a Class C Felony (KRS 434.840-434.860) to access electronically-stored data when you have no right or permission to do so. The felony also applies to those who allow or "cause to be accessed" the same.

It is a Class D Felony (KRS 512.020) to intentionally or unintentionally deface, destroy, or damage any public agency data or technology property.

The responsibility for protecting against loss of OVEC data lies with the individual user. Users must maintain electronic copies of documents on their primary workstation and regularly back those documents up to the network storage server. *Knowledge of this procedure should be considered necessary to the execution of any job duties which employ OVEC technology resources.* It is crucial to understand that there is no fool-proof, fail-safe method of protecting electronic documents; the best possible defense is the vigilance and effort it takes to make multiple copies of important data. Do not maintain only a single copy of a critical file. Do not maintain your only copies on the same storage device or in the same location.

The OVEC network includes an open **\Share** directory which shall be mapped to all domain workstations as drive **G:\** when possible. Its purpose is to serve as a central location for the distribution of files to all OVEC staff, or as a place where users may temporarily place specific files or folders to share them with others for short periods. It should not be considered as an appropriate file backup resource. Confidential information shall not be stored within **\Share**. Alternatively, secure network directories may be supplied by the CTO upon request.

### ***Addition of Workstations and Workstation-Shared Printers***

Users shall not incorporate "power on" passwords orated into the BIOS, CMOS, or other startup feature of any OVEC computer.

No machine running a server operating system may be connected in any way to the OVEC local area network without the approval of the Chief Technology Officer (CTO). Workstation operating systems must be approved by the CTO. Currently approved workstation operating systems are Windows 2000 Professional, Windows XP Professional, and Apple Macintosh OS-X.

The OVEC domain user right to add workstations to the OVEC domain or rename existing workstations is conditional upon the approval of the CTO.

No workstation may be added to the OVEC LAN with a static IP address without approval of the CTO. Instead, use DHCP to assign IP addresses.

Enabling *File/Print Sharing* on individual workstations should be done only when necessary to the execution of job duties; when it is used, do not restrict access through user-assigned passwords without the knowledge and consent of the CTO. In effect, workstation shares must be considered “open” on the local area network (LAN) unless designated otherwise by the CTO.

### ***Addition of Network Printers and Hardware***

With network printers, static IP addresses are the OVEC standard; only the Chief Technology Officer may assign static IP addresses.

The installation and configuration of networked appliances such as network storage devices, network printers, routers, gateways, wireless access points, switches, or additional hubs must be approved by the CTO.

Any security above and beyond OVEC Active Directory security on network devices (network printers, storage appliances, etc.), including administrative passwords for configuration tasks, must be configured by or with the knowledge and approval of the CTO. Passwords and security settings on network printers may not be changed without the knowledge and consent of the CTO.

### ***Workstation Maintenance***

Workstations and individually connected printers should be turned off every evening when employees leave. This does not apply to network printers. Unless configured to power down when the computer is turned off, monitors and desktop printers should manually be turned off every evening as well.

### ***Copyright and Software Licensing***

Software must not be installed, used, or shared between users in violation of an existing software license – software piracy will not be tolerated at OVEC. For questions about a software application license, read and comply with said application’s EULA (End User License Agreement), which will specify whether the rights purchased are for a single user on a single workstation, for multiple users, or for multiple workstations. Software may not be copied or shared outside the provisions of the agreement with the software publisher. Violations of software licensing agreements may constitute serious infractions of federal law and the violator may be subject to civil and/or criminal penalties.

Employees shall not:

- Copy software without authorization from the publisher or copyright holder;
- Use software for which he or she does not have proof of legal right;
- Copy information or programs from the internet and re-use or distribute it without acknowledging authorship and source;

- Assume that he or she can load the older version of software on another workstation after the installation of a software upgrade to the original workstation; and
- Take over a workstation without ensuring that the software already loaded is legal. When you assume responsibility for the workstation, you assume responsibility for the software.

Distributors of software and the Software Publishers Association have the legal right to audit OVEC at any time to ensure compliance with licensing agreements. The user, program under which that user works, or the Technology Office must be prepared to show a software license certificate or copy of the purchase order for each piece of software loaded on that system.

Users must not load software on OVEC computers without notifying the CTO or their program's technology assistant. If the responsible party cannot show proof of license of proper authorization for a software program, OVEC has the right to remove the software from the computer or fileserver.

### ***Prohibited Software***

The following types of software are prohibited on OVEC network client machines without the knowledge and consent of the CTO. OVEC employees are not to install or use any of the following or similar programs on OVEC workstations:

- a. Streaming music or video clients (*Spinner*, radio station clients, etc.)
- b. Instant messaging clients (AOL, *Trillian*, IRC or chat clients, etc.).
- c. Software that requires consent to also install marketing or monitoring software in order to be installed.
- d. "Amusement" applications with no applicability to the employee's job duties. Examples include *BonziBuddy*, *VirtuaGirl*, etc.
- e. Applications that require processing power and/or bandwidth as a condition of discounted or free software. The industry term for this type of program is Grid Programming or Distributed Computing; examples include *Seti@Home*, *ClimatePrediction.net*, etc.
- f. Any software from the company called Claria (formerly called Gator).
- g. Any software associated with GAIN Publishing.
- h. Other known "freeware" or "shareware" applications known to contain spyware, adware, or other bundled applications from partner software corporations.
- i. Games other than those bundled with the operating system. (Instructional games and game-like software being evaluated or reviewed by staff in the course of their jobs are excluded from this prohibition.)
- j. Any software deemed by the CTO as having an adverse impact on the performance of the workstation, server, network, or internet connection.

Applications that monitor, intercept, or decode network information, such as "packet sniffers," password retrievers, or port scanners, are explicitly prohibited on the OVEC LAN except under the approval and supervision of the CTO.

### ***Security Software***

OVEC workstations must run an antivirus application approved by the CTO and should be configured to schedule automatic, regular updates. Such software may be supplied by OVEC at the discretion of the CTO, but if not so supplied must be funded by the funding source of the workstation. Additional security software may be installed or mandated by the CTO. Desktop firewall software should not be installed or enabled unless approved by the CTO.