

**COMPUTER/ON-LINE SERVICES**  
(Acceptable Use and Internet Safety)  
(Employees)

This policy is intended to promote the responsible and ethical use of computer resources by employees in the Wynford Local School District. It covers all computers and computer resources owned, leased, operated or contracted by the District. This includes, but is not limited to, electronic mail and Internet usage, software programs, WynNet, phone systems, microcomputers, minicomputers and mainframes.

The District's network is referred to as "WynNet." Employees may use WynNet for work-related purposes consistent with the mission of the District. Access to all computer resources is a privilege granted to employees. All computer resources and communications transmitted by, received from, or stored in computer systems belong to the District and should not be considered confidential and/or property of the employee.

Employees using the District's computer resources, including electronic mail and the Internet, are responsible for using resources in an authorized, legal and legitimate manner. Technology resources should only be used for work-related purposes and not for personal use. All employees must have an Acceptable Use Policy and Agreement form on file with the school before an employee can access the network, a computer on the network and/or the Internet.

The Wynford School District disclaims responsibility and will not be responsible for loss or disclosure of user information or interference with user information resulting from its efforts to maintain the privacy, security and integrity of the computer and networking facilities and information.

Prohibited Conduct

Employees must adhere to the following rules when using the District's technology resources, including the Internet:

1. Technology resources, including electronic mail and the Internet, must not be used by employees for product advertising or for commercial or political purposes. Technology resources may only be used for legitimate work-related purposes within the course and scope of the employee's duties. WynNet, including the Internet and electronic mail, may not be used in connection with compensated outside work, to complete personal coursework during scheduled teaching assignments or for the benefit of organizations not affiliated with the District.
2. All policies, including the sexual harassment policy, apply to the use of computer resources. Employees are prohibited from engaging in any conduct and/or behavior that constitutes any form of harassment, including sexual harassment, through the use of computer resources and/or communication systems. This includes sending harassing or libelous electronic mail or computer messages to others over the WynNet. It also includes sending, access and/or displaying harassing jokes, cartoons, inappropriate website addresses or material of a similar nature.

If an employee receives offensive or harassing material from others over the WynNet, the employee should immediately notify the systems administrator or the Superintendent.

Employees are specifically prohibited from using the Internet and other school technology resources to download, access or send pornographic, lewd, offensive, indecent, obscene or vulgar materials.

3. Employees granted access to confidential records, of students or other employees, have the important responsibility of maintaining the confidentiality of information and may be disciplined for sharing or releasing information to others without authorization. Information that is considered confidential should not be sent to a network printer without an authorized person available to safeguard its confidentiality during and after printing.
4. The willful wasting of computer and networking facilities resources is considered inappropriate use. Wastefulness includes, but is not limited to, passing chain letters, generation of large volumes of unnecessary or non-work related printed output or disk space, or creation of heavy network traffic such as streaming radio or video for non-education purposes.
5. Employees are prohibited from negligently and/or intentionally damaging, destroying or altering school technology resources in any unauthorized or illegal manner (i.e., computer hacking, uploading/creating viruses, etc.) Any malicious attempt by an employee to harm or destroy data that is connected to the WynNet is specifically prohibited.
6. Web sites using the name “Wynford” or referring to the District in any way may only be developed and maintained by authorized personnel. Staff must consult the systems administrator prior to publishing the web page and must follow the guidelines established by the District.
7. Personal calls on the school’s telephone systems are to be limited to urgent or emergency use. The use of mobile phones paid for by the District can be monitored for inappropriate call patterns, unexpected costs and excessive personal use.
8. Employees may not alter the settings that are placed on the computer including, but not limited to, the following: any web browser preference or Internet option settings, any settings found in the network properties, e-mail settings other than username or any personalization of computer equipment including, but not limited to: wallpaper, screen savers, pointers or sounds etc. that interferes with the performance or maintenance of the computer.
9. Users agree to indemnify the District for any loss or damage arising out of improper use.
10. Employees may not use technology resources to conduct illegal activity that would violate State, Federal or local law, or any other school policy.

### Access Issues

The District reserves the right to; monitor, access, inspect, intercept and take appropriate action with respect to all technology resources and communications. Common examples of when the District may need to access computers, software or stored communications in include: investigation of suspected misuse of the computer or Internet; conducting system repairs or any other legitimate purpose in accordance with school policy or Federal, State or local law. Employees cannot access or retrieve stored communications unless authorized to do so by the systems administrator or Superintendent.

The District also reserves the right to search and seize computer resources used by employees, such as computer, disks, electronic mail messages, Internet materials, etc. The search will be conducted at the discretion of the District, and the systems administrator will be involved in all searches.

### Internet and Electronic Mail

The Internet and electronic mail system are to be used by employees for legitimate, school-related purposes only. Sending electronic “chain-letters” does not constitute legitimate use of the computer resources.

The District will use software filters and other techniques whenever possible to restrict access to inappropriate information on the Internet.

Electronic mail is not confidential and privileged. Because the District owns the computers, electronic mail communications, whether sent or received by the district, are considered the property of the District. Employees using electronic mail do so at their own risk.

Unsolicited e-mail is to be treated with caution and not responded to. Electronic files received from unknown senders are to be deleted without being opened.

### Files Stored on the District’s Server and/or on the District’s Computers

Employee files stored on the District’s server must be for educational purposes only. No executable files or non-school related files (including pictures) are to be in an employee’s folder. If such files are found on the server or on a District computer, they will be deleted immediately and the infraction will be reported to the employee’s supervisor.

Files in an employee’s folder are property of the District and may be reviewed without notification. When an employee leaves the District, all employee files will be deleted and the password will be revoked.

Employees are expected to periodically clean files off of the server, including e-mail server, and are to remove those files that are no longer necessary.

### Software

Federal copyright laws protect computer software, and employees are prohibited from engaging in unauthorized duplication, distribution or alteration of any licensed software. Employees must abide by all software licensing agreements and may not illegally use or possess copyrighted software. Employees must not use software that they know has been illegally copied. Software purchasing and installation should be done in conjunction with the systems administrator in all cases.

Network license software is typically used by a limited number of concurrent users. However, unless permitted by the license, this software must not be copied from the server to the employee’s individual workstation.

Site license can be used on any equipment at the site for which the software is purchased. This software can be legally copied onto any site that holds the license. However, unless permitted by the license, it must not be copied to equipment not owned by the license.

Single license software must not be copied to multiple machines or media in violation of the license agreement. However, employees may bring personal single license software to install on the school’s computer resources in the following circumstances:

1. The user has gained permission from the systems administrator to install the software.
  - A. Permission will only be granted to install software that is educationally based, that is used by students and is deemed appropriate for school use.
  - B. Software that is found on a machine that has not had permission granted will be uninstalled immediately.
2. The user can prove ownership (i.e., license agreement).
3. The user adheres to the licensing and copyright agreements for the software.
4. The user has registered the software with the software company.

The guidelines stated above also pertain to the downloading and installation of software from the Internet. Before installing software, whether purchased or downloaded, the systems administrator must grant permission.

### Security

Computer security is a high priority for the District. If an employee identifies a security problem on the Internet or other technology resources, the employee must notify the systems administrator or the Superintendent.

Employees must keep their account and password information confidential, private and may not share it with others. Employees are prohibited from using another individual's account and/or password. Approved login procedures must be strictly observed and users leaving a computer unattended must first log off. Employees are also prohibited from using a personal code not registered with the system administrator when using technology resources.

The District will not be liable for lost or damaged data stored on the technology resources of the school by employees, nor for security violations committed by employees.

### Discipline

Employees violating the terms and conditions of this policy will be subject to discipline up to and including termination of employment. Violation of this policy may also result in the revocation and/or suspension of the employee's access/using rights.

Employees may be disciplined for conduct and/or behavior associated with the prohibited use of technology resources which occurs on work time, or for conduct which occurs outside of work time but directly relates to and/or affects the District, students and staff. Employees will also be disciplined for using computer resources in a manner which harms or intends to harm school property, employees and/or students.

Questions about this policy should be addressed to the systems administrator or the Superintendent.

[Adoption date: June 17, 2002]

Wynford Local School District, Bucyrus, Ohio

**COMPUTER NETWORK AGREEMENT FORM**

I hereby apply for an employee account on the District computer network: (please print clearly)

Name \_\_\_\_\_

School \_\_\_\_\_

Home Address \_\_\_\_\_

City/State/Zip \_\_\_\_\_

Home Phone \_\_\_\_\_

I have read and I understand this computer policy and its guidelines and regulations and agree to abide by all of the rules and standards for acceptable use state therein. Should I commit any violation or in any way misuse my access to the District's computer network and the Internet, I understand and agree that my access privilege may be revoked and disciplinary action may be taken against me. I further state that all information provided for the creation of this account is truthful and accurate.

Signature \_\_\_\_\_ Date \_\_\_\_\_