

Chittenden Central Supervisory Union  
**Procedure: Technology Acceptable Use for Employees**  
**File Code: G2E-R**

*Revised: 12/1/09*

The following technology acceptable use and standards of conduct shall apply to:

1. Users of electronic information resources which are utilized with equipment located or accessed in the District.
2. Users who obtain their access privileges through association with the District.

Personal Responsibility: Users are expected to:

1. Use electronic information resources in support of education, research and the educational goals and objectives of the District, except as otherwise allowed under CCSU policy (G2E).
2. Promote acceptable use of the electronic information resources and network etiquette and report any misuse of the network to the Network Administrator. Misuse can come in many forms, but it is commonly viewed as any material sent or received that indicates or suggests pornography, unethical or illegal behavior, racism, sexist, inappropriate language, or violation of other issues as described below.
3. Supervise students using electronic information resources, and report any misuse to the Network Administrator as necessary.
4. Refrain from using the network for commercial purposes.
5. Remove unwanted and unused files regularly.
6. Refrain from using district-provided technologies for product endorsement, political lobbying, or private business or enterprise purposes.
7. Refrain from uploading, downloading or redistributing public domain programs to the system for personal use without advance permission from the Network Administrator.

Network Etiquette: Any user is expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to, the following:

1. Be polite. Never send or encourage others to send abusive, harassing, or threatening messages.
2. Use appropriate language. Do not swear, use vulgarities, or any other inappropriate language.
3. Refrain from transmitting any material in violation of any federal or VT state statute or regulation is prohibited (e.g. copyrighted material, threatening of obscene material, or material protected by trade secret, etc.) Illegal activities are strictly forbidden.
4. Protect your personal information and personal information of others. Do not transmit personally identifiable confidential information about yourself or others (e.g. information protected under the Family Education Rights and Privacy Act (FERPA) and CCSU *Procedure: JOB-R*, social security numbers, HIPAA protected medical information, etc.).
5. Do not use the network in such a way that you would disrupt the use of the network by other users.
6. Never submit, publish, display, or retrieve, any defamatory, abusive, obscene, profane, sexually oriented, threatening, racially offensive, harassing, or illegal material.
7. Abide by all copyright regulations when using technology.

Privacy: Note that electronic mail (e-mail) is not guaranteed to be private. People who operate the system can and do have access to all e-mail. E-mail history may be made available to the Superintendent and/or his/her designee upon request for the purpose of investigation or complying with requests for public information. Messages relating to or in support of illegal activities will be reported to the authorities. All communication and information accessible via the network should be assumed to be District property.

Security: Security on any computer system is a high priority, especially when the system involves many users. If a user identifies a security problem on the Local Area Network (LAN), the user must notify the Help Desk, Network Administrator

or other technology staff person, and should not demonstrate the problem to other users. Nor should another individual's account be used without written permission from that individual.

- Employees are responsible for the proper use of their account, including password protection.
- Employees shall take all reasonable precautions, including password maintenance and file and directory protection measures, to prevent the use of his/her account by unauthorized persons.

Vandalism: Vandalism of district technology or other electronic information is strictly prohibited. Vandalism is defined as any malicious attempt to access, harm, modify or destroy data of another user, LAN, Internet, or any agencies or other networks that are connected to the Internet backbone. Vandalism shall also include any malicious intent to harm, modify, or destroy hardware of software, or interfere with system security.

No guarantees: The District makes no warranties of any kind, whether expressed or implied, for the service it is providing. The District will not be responsible for any damages suffered. This includes loss of data resulting from delays, non-deliveries, mis-deliveries, service interruptions, changes, or consequences arising therefrom, caused by its own negligence or the users errors or omissions. Use of any information obtained via the Internet is at the user's own risk. The District specifically denies any responsibility for the accuracy or quality of information obtained through its Internet services.

Restrictions/limitations: The following restrictions/limitations shall apply to the electronic information resources and applicable services provided through the District:

- The District reserves the right to log the use of all systems and monitor fileserver space utilization. Should it become necessary, files may be deleted.
- The District reserves the right to establish such rules and regulations as may be necessary to maintain the operation of the electronic information systems.
- Many services and products are available for a fee. Users are responsible for any expenses incurred while using electronic information resources.

Consequences: Infractions of the provisions set forth herein may result in appropriate disciplinary action. Inappropriate behavior in violation of state and federal statutes will be subject to prosecution by those authorities. The administration may also request the Network Administrator to deny, limit or suspend access to specific user accounts.