

Valmeyer Community Unit School District #3

Acceptable Use

Of

Computers and Networks

The Valmeyer Community Unit School District #3 Board of Education supports the use of the Internet and other computer networks in the district's instructional program in order to facilitate learning and teaching through interpersonal communications, access to information, research, and collaboration.

The use of network facilities shall be consistent with the curriculum adopted by the school district as well as the varied instructional needs, learning styles, abilities, and developmental levels of students.

The Board expects all Faculty, Students, Staff, and Associates to use the District's Computers and Networks responsibly. All computing resources must be used in an Effective, Ethical, and in a Lawful manner. Users are expected to learn and follow normal standards of polite conduct and responsible behavior in their use of computer resources.

Responsibility

The district shall make every effort to ensure that this educational resource is used responsibly by students and staff. Administrators, teachers and staff have a professional responsibility to work to help students develop the intellectual skills necessary to discriminate among information sources, to identify information appropriate to age and developmental levels, and to evaluate and use the information to meet their educational goals.

The students and staff have the responsibility to respect and protect the rights of every other user in the district and on the Internet. The building administrator shall have the authority to determine what inappropriate use is, and his/her decision is final. The district network and access to the Internet exist for the primary purpose of transmitting and sharing information between Academic Organizations. It is the responsibility of each user on the district network or the Internet to recognize his/her accountability in having access to these vast services, sites, systems and people, and to act according to acceptable behavior standards when using them.

There should be no expectation of privacy in any use of E-mail, internet access, or use of the district's network as a whole. Any and all computers or other devices (I.E. PDAs or Cell Phones) that are connected directly or wirelessly to the district's network infrastructure are subject to inspection and monitoring at any time by district technology or administrative personnel. Random remote monitoring may be done without any indication or notice to any user at any time via; Virtual Network Connection (VNC), packet sniffing, or other means may be employed. Computer files and even deleted files not erased may be accessed and read at any time for monitoring and policy enforcement purposes by authorized personnel.

Authority

- A. The electronic information available to students does not imply endorsement of the content by the school district, nor does the district guarantee the accuracy of information received on the Internet.
- B. The district shall not be responsible for any information that may be lost, damaged, or unavailable when using the network or for any information that is retrieved via the Internet.
- C. The school district shall not be responsible for any unauthorized charges or fees resulting from access to the Internet.
- D. The district reserves the right to log network use and to monitor file server space utilization by district users.
- E. The Board establishes that the use of the Internet is a privilege, not a right. Inappropriate, unauthorized, or illegal use will result in the cancellation of those privileges and appropriate disciplinary action.

RULES AND PROCEDURES FOR USE OF COMPUTER RESOURCES

I. Use of Computer Hardware

- A. Computer hardware is like any other School property and shall be treated accordingly. All desktop computers, laptops, and cell phones provided by the District remain the property of the school district. All items must be made available for inventorying, inspection, updating, and or maintenance at any time by the district technology or administrative personnel at any time.
- B. Only authorized Individuals will install, service, and/or maintain district-owned computer hardware.
- C. No hardware, including cables or peripherals may be moved, removed from the district, or loaned to another district employee without authorization from the technology director.
- D. It is the responsibility of the faculty/staff member to whom the computer is assigned to log off and shut down the computer and all peripherals at the end of each day. It is the responsibility of the faculty, students, and staff, to keep the computers clean and free of dust, magnets, food, liquid, or any other foreign material known to be harmful to the hardware or functionality of the system.
- E. It is the responsibility of the faculty/staff member to whom the computer is assigned, to report malfunctions of the hardware or software to the technology director by means of the electronic form provided on the District web page.
- F. No privately owned computers, laptops, or palm computers may be introduced to the District network without the permission of the technology director. Such equipment approved must be presented for inspection and/or monitoring at the request of the technology director or administrator.

II. Use of Computer Software

- A. Only software (on disk or downloaded) that is legally owned and/or authorized by the district may be installed on district computers.
- B. The unlawful copying of any copyrighted software and/or its use on district hardware is prohibited.
- C. Modification, removal, or erasure of any software without authorization is prohibited.
- D. The intentional introduction of any viral agent(s) is prohibited. All externally used diskettes or “thumb” (USB) drives should be checked for viruses each time they are put into or connected to a district-owned computer system.
- E. Any individual who intentionally introduces a virus into the district system or violates the copyright laws shall be subject to appropriate district discipline policies and to the penalty provisions of the AUP.
- F. The technology director and/or the building administrators have the right and responsibility to remove any software from district-owned equipment where the user cannot provide original copies of the software and/or appropriate license for the software.

III. Use of Remote Communications and the Computer Network

- A. All computers for Student use from which the Internet and shared resources can be accessed will be in supervised areas. School district staff shall monitor student computer use, providing assistance, or taking corrective action when necessary. Any student found using a machine unsupervised will be subject to appropriate district discipline policies and to the penalty provisions of the AUP.
- B. Network use must be consistent with the goals and standards of the district, school, and specific curriculum.
- C. Networked computers may be used for research, experimentation in computer communications, and curriculum development where such use does not interfere with normal operations.
- D. Others must not use an account assigned to an individual, including student use accounts. Faculty, students, staff and associates are individually responsible for the proper use of their accounts, including proper password protection and appropriate use of network resources.
- E. Use of any login and password by any user through Telnet or FTP resources from district computers is prohibited without authorization from the Technology Director.
- F. Use of sites such as MySpace, FaceBook, or You Tube is prohibited unless there is a valid educational benefit to be gained by doing so. Staff members may request use through their respective principal and the technology director.

IV. Behavior Standards

A. Though the district uses an Internet filter that blocks inappropriate sites, no filter is perfect.

Accessing or attempting to access inappropriate Internet sites is prohibited.

Inappropriate Internet sites can be, but are not limited to:

- Sites containing pornographic and other objectionable materials.
- Sites using obscene language.
- Sites encouraging hatred or terrorist acts.
- Sites that enable and encourage circumvention of the district's internet filter
- File sharing sites that encourage illegal downloading of copyrighted materials such as music, books, or video/motion pictures

B. Abusive conduct when using district computers or the network is prohibited.

Abusive conduct can be, but is not limited to:

- Placing of unlawful information on any computer system.
- Using abusive, obscene, threatening or objectionable language through email, social networking or any other means.
- Sending messages that are likely to result in the loss of recipient's work or systems.
- Sending "chain letters" or "broadcast" messages to lists or individuals.
- Use of the system to intimidate or create an atmosphere of harassment.

C. Interference with or disruption of the network users, services, or equipment is prohibited.

Disruptions can include, but are not limited to:

- Distribution of unsolicited advertising.
- Propagation of computer worms or viruses.
- Unauthorized entry to any other machine accessible via the network.
- Attempting to degrade or degrading computer or network system performance.
- Transmission of any material in violation of any U.S. or State Laws or Regulations is prohibited and may constitute a criminal offense.
- Accessing another individual's E-mail is prohibited, except when an investigation requires the monitoring of systems by the technology director or the administration.
- Attempts to gain unauthorized access to remote systems are prohibited.
- The use of another individual's access codes/passwords is prohibited.
- Copying of another individual's work or copyrighted material is prohibited.

General Policies

- A. The network user shall be responsible for damages to equipment, systems and software resulting from deliberate or willful acts.
- B. Illegal use of the network, intentional deletion or damage to files of data belonging to others, copyright violation, or theft of services will be reported to the appropriate legal authorities for possible prosecution.
- C. General rules for behavior and communications apply when using the Internet, in addition to the stipulations of this policy. Penalties for flagrant misuse of the Internet may include, but are not limited to, loss of Internet access and/or computer use and other disciplinary actions for a stipulated period of time.
- D. Vandalism will result in cancellation of access privileges. Vandalism is defined as any malicious attempt to harm or destroy data of another user, Internet or other networks. This includes, but is not limited to, the uploading or creation of computer viruses
- E. All users of district equipment must sign the appropriate District Computer and Network AUP Agreement stating they understand all policies regarding computer use and agree to abide by them. Network access will not be given to a user until he/she has agreed to, and signed this policy.
- F. Any and all equipment district owned is subject to these rules and provisions when connected to the district network, including provisions for inspection and remote monitoring. Any form of remote connection from within or outside the school district, while connecting to computer resources inside the district are subject to these same rules and provisions. Connections may be made physically, wirelessly, or in any other fashion.
- G. Personally owned computers, laptops or other communications equipment may not be connected to the district network without consent from the technology office and is subject to the same rules and provisions for inspection and monitoring as district owned equipment.
- H. Any other party cannot hold the district liable for any losses, including lost revenues or for any claims or demands against the user. The district cannot be held responsible for any damages due to the loss of output, loss of data, time delay, system performance, software performance, incorrect advice, or any other damages arising from the use of the district's computer facilities and network.
- I. The individual user and/or their Parent or Guardian in the case of a Student, will be held liable for any of the above issues that he/she causes or policies that are violated.
- J. In accordance with the expectation that all computing resources being used in an Effective, Ethical, and Lawful manner, the following uses are specifically prohibited:
 - Use of the network to facilitate illegal activities
 - Use of the network for commercial or for-profit purposes
 - Use of the network for non-work or non-school related work

- Use of the network for product advertisement or political lobbying
- Use of the network for hate mail, discriminatory remarks, or offensive or inflammatory communication
- Use of the network to intentionally obtain or modify files, passwords and data belonging to others
- Use of the network to disrupt the work of other users
- Use of the network to access obscene or pornographic material
- Use of the network facilities for fraudulent, unauthorized or illegal installation, distribution, reproduction, modification, or use of copyrighted materials
- Loading or use of unauthorized games, programs, files or other electronic media
- Use of inappropriate language or profanity on the network
- Destruction, modification or abuse of network hardware or software
- Impersonation of another user, anonymity or pseudonyms
- Quoting personal communications in a public forum without the original authors prior consent

E-mail

Students in grades 6-12 will be provided with an E-mail account. The use of the school email account is limited to school related activities and communications between students and their parents/guardians. Since the district is providing an E-mail account, use of any other E-mail accounts or online communication is strictly forbidden. This includes the use of chatting software such as AOL Instant Messenger, Yahoo Messenger, and the like. Inappropriate use of the account will result in disciplinary action.

Proper Respect for Copyright

In an effort to encourage the proper respect for copyright on the Internet, the following guide for Student users is provided:

- If the user did not create a non-public domain written work, piece of art, photograph or music, or obtain rights to it, the user does not own it!
- If the user does not own the non-public domain material, the user may not copy it or distribute it to others.
- The author or owner of a document or other type of information must explicitly relinquish rights in order to place a work in the "Public Domain" and thereby make copying/distribution with specific authorization possible.

- “*Fair use*” allows the user to copy small portions of a work the user does not own without permission, but only for Criticism, Education, News Reporting, and the like there of. Any copies must then be destroyed or erased.
- When in doubt, the user should ask the creator or owner of material for permission to use the work.

Brian D. Charron
Superintendent
Valmeyercommunity Unit School District #3

Computer and Network Faculty/Staff Agreement

As an employee of Valmeyer Community Unit School District 3, I agree to follow the District Computer and Network Acceptable Use Policy Agreement and its behavioral standards. I agree to take care of the equipment assigned to me, protect them from foreign materials, and maintain and update my equipment when necessary and within my abilities.

I understand that I will be given network and Internet privileges that students may or may not have. I agree to regularly monitor students while they are using the computers and network. If I allow student(s) access to the Internet through my own login and password, I agree to take responsibility for monitoring the student while they are using the computer.

I agree to maintain security on my computer and the district network, and account by not giving out my password or any other password deemed for "Faculty/Staff only". I understand that I should not write down my password, but rather make my password something I can remember. I also understand that my hard drive (C :) could crash or need to be replaced at any time, and that I should save all important personal and school related data to my folder on the server, CD, or a "Thumb" (USB) Drive.

I have read, understand, and agree to follow all policies outlined in the Valmeyer Community Unit School District 3 Computer and Network Acceptable Use Policy Agreement as well as promote this agreement with the students. I understand that the computers and network are to be used for Educational purposes. I agree to use the network in accordance with the policy and model to my student's proper network etiquette. I also agree to report any misuse or suspicion of misuse of electronic information to the proper authorities.

I understand that if I violate the District Computer and Network Acceptable Use Policy Agreement, some or all of my computer and/or network privileges could be revoked. I also understand that I am subject to all appropriate disciplinary measures found in the district policies should these guidelines be violated.

Faculty/Staff Name: _____

Signature: _____

Building (Room/Office): _____

Date: _____

***Keep a copy of this Agreement for your records! Give the original to the technology director.**

Board Approved: August 18, 2008