REGULATION

VERNON TOWNSHIP
BOARD OF EDUCATION

PROGRAM
R 2361/Page 1 of 7
Acceptable Use of Computer
Network/Computers and Resources
Apr 05
Sept 12
M

R 2361 ACCEPTABLE USE OF COMPUTER NETWORK/COMPUTERS AND RESOURCES

For the purpose of this Policy and Regulation, "computer networks/computers" includes, but is not limited to, the school district's computer networks, computer servers, computers, other computer hardware and software, Internet equipment and access, and any other computer related equipment.

For the purpose of this Policy and Regulation, "school district personnel" shall be the person(s) designated by the Superintendent of Schools to oversee and coordinate the school district's computer networks/computer systems. School district personnel will monitor networks and online activity, in any form necessary, to maintain the integrity of the networks, ensure proper use, and to be in compliance with Federal and State laws that regulate internet safety.

Due to the complex association between government agencies and computer networks/computers and the requirements of Federal and State laws, the end user of these computer networks/computers must adhere to strict regulations. Regulations are provided here so that staff, community, and pupil users and the parent(s) or legal guardian(s) of pupils are aware of their responsibilities. The school district may modify these regulations at any time by publishing modified regulations on the network and elsewhere. The signatures of the pupil and his/her parent(s) or legal guardian(s) on the district-approved consent and waiver agreement are legally binding and indicate that the parties have read the terms and conditions carefully, understand their significance, and agree to abide by the rules established under Policy and Regulation No. 2361.

Pupils are responsible for ~~good~~ behavior acceptable and appropriate and conduct on computer networks/computers just as they are in a classroom or a school hallway. Communications on the computer network/computers are often public in nature. Policies and Regulations governing behavior and communications apply. The school district's networks, Internet access and computers are provided for pupils to conduct research and communicate with others. Access to computer network services/computers is given to pupils who agree to act in a considerate and responsible manner. Parent permission is required. Access entails responsibility. Individual users of the district computer network/computers are responsible for their behavior and communications over the computer network/computers. It is presumed that users will comply with district standards and will honor the agreements they have signed.

Beyond the clarification of such standards, the district is not responsible for the actions of individuals utilizing the computer network/computers who violate the policies and regulations of the Board.

Computer network/computer storage areas shall be treated in the same manner as other school storage facilities. School district personnel may review files and communications to maintain system integrity and confirm users are using the system responsibly. Users should expect that files stored on district servers will be private or confidential.

The following prohibited behavior and/or conduct using the district's networks/computers, includes but is not limited to the following:

1. Sending or displaying offensive messages or pictures;

2. Using obscene language and/or accessing visual depictions that are obscene as defined in section 1460 of Title 18, United States Code;

3. Using or accessing visual depictions that are child pornography, as defined in section 2256 of Title 18, United States Code;

4. Using or accessing visual depictions that are harmful to minors including any pictures, images, graphic image file or other visual depiction that taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; or

5. Depicts, describes, or represents in a patently offensive way, with respect to what is suitable for minors, sexual acts or conduct; or taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors;

6. Cyberbullying;

7. Inappropriate online behavior, include inappropriate interaction with other individuals on social networking sites and in chat rooms.

8. Harassing, insulting or attacking others;

9. Damaging computers, computer systems or computer network/computers;

10. Violating copyright laws;

11. Using another's password;

12. Trespassing in another's folders, work or files;

13. Intentionally wasting limited resources;

14. Employing the computer network/computers for commercial purposes; and/or

15. Engaging in other activities that do not advance the educational purposes for which computer Network/computers are provided.

INTERNET SAFETY

Compliance with Children's internet Protection Act

As a condition for receipt of certain Federal funding, the school district has technology protection measures for all computers in the school district, including computers in media centers/libraries, that block and/or filter material or visual depictions that are obscene, child pornography and harmful to minors as defined in 2, 3, 4, 5, 6 and 7 above and in the Children's internet Protection Act. The school district will certify the schools in the district, including media centers/libraries are in compliance with the Children's internet Protection Act and the district enforces Policy 2361.

Compliance with Neighborhood Children's Internet Protection Act

Policy 2361 and this Regulation establishes an Internet safety policy and procedures to address:

1. Access by minors to inappropriate matter on the Internet and World Wide Web;

2. The safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications;

3. Unauthorized access, including "hacking" and other unlawful activities by minors online;

4. Cyberbullying;

5. Inappropriate online behavior including inappropriate interaction with other individuals on social networking sites and in chat rooms;

6. Unauthorized disclosures, use, and dissemination of personal identification information regarding minors; and

7. Measures designed to restrict minors' access to materials harmful to minors.

Notwithstanding the material or visual depictions defined in the Children's internet Protection Act and the Neighborhood Children's Internet Protection Act the Board shall determine Internet material that is inappropriate for minors. The Board will provide reasonable public notice and will hold one annual public hearing during a regular monthly Board meeting or during a designated special Board meeting to address and receive public community input on the Internet safety policy – Policy and Regulation 2361.

Information Content and Uses of the System

Pupils may not publish on or over the system any information which violates or infringes upon the rights of any other person or any information which would be abusive, profane or sexually offensive to a reasonable person, or which, without the approval of the Superintendent of Schools or designated school district personnel, contains any advertising or any solicitation to use goods or services. A

pupil cannot use the facilities and capabilities of the system to conduct any business or solicit the performance of any activity, which is prohibited by law.

Because the school district provides, through connection to the Internet, access to other computer systems around the world, pupils and their parent(s) or legal guardian(s) understand that the Board and school district personnel have no control over content. While most of the content available on the Internet not offensive and much of it a valuable educational resource, some objectionable material exists. The Board provides pupils access to Internet resources through the district's computer network/computers with installed appropriate technology protection measures, parents and pupils must be advised potential dangers remain and offensive material may be accessed notwithstanding the technology protection measures taken by the school district. Pupils and their parent(s) or legal guardian(s) are advised that some systems may contain defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, or otherwise illegal material. The Board and school district personnel do not condone the use of such materials and do not permit usage of such materials in the school environment. Parent(s) or legal guardian(s) having Internet access available to their children at home should be aware of the existence of such materials and do not permit usage of such material in the school environment. Pupils knowingly bringing such materials into the school environment will be disciplined in accordance with Board policies and regulations and such activities may result in termination of such pupils' accounts on the computer network and their independent use of computers.

On-line Conduct

Any action by a pupil or other user of the school district's computer network/computers that is determined by school district personnel to constitute an inappropriate use of computer network/computers resources or to improperly restrict or inhibit other members from using and enjoying those resources is strictly prohibited and may result in limitation on or termination of an offending person's access and other consequences in compliance with Board policy and regulation. The user specifically agrees not to submit, publish, or display any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, or otherwise illegal material; nor shall a user encourage the use, sale, or distribution of controlled substances. Transmission of material, information or software in violation of any local, state or federal law is also prohibited and is a breach of the Consent and Waiver Agreement.

Pupils and their parent(s) or legal guardian(s) specifically agree to indemnify the Vernon Township School District and school district personnel for any losses, costs, or damages, including reasonable attorneys' fees incurred by the Board relating to, or arising out of any breach of this section by the pupil.

Computer network/computer resources are to be used by the pupil for his/her educational use only; commercial uses are strictly prohibited.

Software Libraries on the Network

Software libraries on or through the networks are provided to pupils as an educational resource. No pupil may install, upload, or download software without the expressed consent of the appropriate administrator. Any software having the purpose of damaging other members' accounts on the school district computer network/computers (e.g., computer viruses) is specifically prohibited. School district personnel further reserve the rights to refuse posting of files and to remove files. School district personnel further reserve the right to immediately limit usage or terminate the account or take other action consistent with the Board's policies and regulations of a member who misuses the software libraries.

Copyrighted Material

Copyrighted material must not be placed on any system connected to the computer network/computers without authorization. Pupils may download copyrighted material for their own use in accordance with Policy and Regulation Nos. 2531, Copying Copyrighted Materials. Any pupil may only redistribute a copyrighted program with the expressed written permission of the owner or authorized person. Permission must be specified in the document, on the system, or must be obtained directly from the author or authorized source.

Public Posting Areas (Message Boards/Blogs, etc.)

Messages are posted from systems connected to the Internet around the world and the school district personnel have no control of the content of messages posted from these other systems. To best utilize system resources, school district personnel will determine which message boards, blogs, etc. that are most applicable to the educational needs of the school district and will permit access to these sites through these the school district computer network. School district personnel may remove messages that are deemed to be unacceptable or in violation of the Board policies and regulations. School district personnel further reserve the right to immediately terminate the access of a pupil who misuses these public posting areas.

Real-time, Interactive, Communication Areas

School district personnel reserve the right to monitor and immediately limit the use of the computer network/computers or terminate the account of a member who misuses real-time conference features (talk/chat/Internet relay chat).

Electronic Mail

Electronic mail ("E-mail") is an electronic message sent by or to a person in correspondence with another person having Internet mail access. All messages sent and received on the school district computer network must have an educational purpose and are subject to review. Messages received by a district-provided email account are retained on the system until deleted by the recipient or for a period of time determined by the district. A canceled account will not retain its E-mail. School district personnel may inspect the contents of E-mail sent by one member to an addressee, or disclose such contents to other than the sender or a recipient when required to do so by the Board policy,

regulation or other laws and regulations of the State and Federal governments. The Board reserves the right to cooperate fully with local, state, or federal officials in any investigation concerning or relating to any E-mail transmitted on the school district computer network/computers.

Disk Usage

The district reserves the right to establish maximum storage spaces a pupil receives on the system. A pupil who exceeds his/her quota of storage space will be advised to delete files to return to compliance with predetermined quotas.

Security

Security on any computer system is a high priority, especially when the system involves many users. If a pupil identifies a security problem on the computer network, the pupil must notify an appropriate school district staff member. The pupil should not inform other individuals of a security problem. Passwords provided to pupils by the district for access to the district's computer network or developed by the pupil for access to an Internet site should not be easily guessable by others, or shared with other pupils. Attempts to log in to the system using either another pupil's account may result in termination of the account. A pupil should immediately notify school district personnel if a password is lost or stolen, or if they have reason to believe that someone has obtained unauthorized access to their account. Any pupil identified as a security risk will have limitations placed on usage of the computer network/computers or may be terminated as a user and be subject to other disciplinary action.

Vandalism

Vandalism to any school district owned computer or network will result in cancellation of system privileges and other disciplinary measures in compliance with the District's discipline code. Vandalism is defined as any malicious attempt to harm or destroy data of another user, the system, or any of the agencies or other computer network/computers that are connected to the internet backbone or of doing intentional damage to hardware or software on the system. This includes, but is not limited to, the uploading or creation of computer viruses.

Printing

The printing facilities of the computer network/computers should be used judiciously. Unauthorized printing for other than educational purposes is prohibited.

Internet Sites and the World Wide Web

Designated school district personnel may establish an Internet site(s) on the World Wide Web or other Internet locations. Such sites shall be administered and supervised by designated school district personnel, who shall ensure the content of the site complies with the federal, state and local laws and regulations as well as Board policies and regulations.

Violations

Violations of the Acceptable Use of Computer Network/Computers and Resources may result in a loss of access as well as other disciplinary or legal action. Disciplinary action shall be taken as indicated in Policy and Regulation Nos. 2361, Acceptable Use of Computer Network/Computers and Resources, No. 5600, Pupil Discipline, No. 5610, Suspension and No. 5620, Expulsion as well as possible legal action and reports to the legal authorities and entities.

Determination of Consequences for Violations

The particular consequences for violations of this policy shall be determined by the Building Principal or designee. The Superintendent or designee and the Board shall determine when school expulsion and/or legal action or actions by the authorities are the appropriate course of action.

Individuals violating this policy shall be subject to the consequences as indicated in Regulation No. 2361 and other appropriate discipline, which includes but is not limited to:

1. Use of Computer Network/Computers only under direct supervision;

2. Suspension of network privileges;

3. Revocation of network privileges;

4. Suspension of computer privileges;

5. Revocation of computer privileges;

6. Suspension from school;

7. Expulsion from school; and/or

8. Legal action and prosecution by the authorities.

Issued: 21 April 2005
Revised: September 2012