

REGULATION GUIDE

RIVER VALE BOARD OF EDUCATION
PROGRAM

Page 1 of 7

R2361 Acceptable Use of Computer Network/
Computers and Resources

R2361 ACCEPTABLE USE OF COMPUTER NETWORK/COMPUTERS AND RESOURCES

The school district provides computer equipment, computer services, and Internet access to its pupils and staff for educational purposes only. The purpose of providing technology resources is to improve learning and teaching through research, teacher training, collaboration, dissemination and the use of global communication resources. The “system administrators” referred to herein as employees of the school district who administer the school district computer network/computers and the system administrators reserve the right to monitor all activity on network/computer facilities/computers.

Because of the complex association between so many government agencies and computer networks/computers, 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 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 is a privilege--not a right. 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. Computer network/computer administrators may review files and communications to maintain system integrity and ensure that users are using the system responsibly. Users should not expect that files stored on district servers will always be private.

R2361 Acceptable Use of Computer Network/Computers
And Resources

Within reason, freedom of speech and access to information will be honored. During school, teachers of younger pupils will guide them toward appropriate materials. Outside of school, families bear the same responsibility for such guidance as they exercise with information sources such as television, telephones, movies, radio and other potentially offensive media. As outlined in Board policy and procedures on pupil rights and responsibilities, copies of these are available in school offices. Behavior including but not limited to the following are prohibited:

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. Harassing, insulting or attacking others;
7. Damaging computers, computer systems or computer network/computers;
8. Violating copyright laws;
9. Using another's password;
10. Trespassing in another's folders, work or files;
11. Intentionally wasting limited resources;
12. Employing the network/computers for commercial purposes; and/or
13. 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

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 visual depictions that are obscene, child pornography and harmful to minors as defined in 2, 3, and 4 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. Unauthorized disclosures, use, and dissemination of personal identification information regarding minors; and
5. Measures designed to restrict minors access to materials harmful to minors.

Notwithstanding the visual depictions defined in the Children's Internet Protection Act and as defined in 2, 3, and 4 above, 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

Users agree not to 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 an average person, or which, without the approval of the system administrators, contains any advertising or any solicitation of other members to use goods or services. The user agrees not to 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 system administrators have no control over content. While most of the content available on the Internet is innocuous and much of it a valuable educational resource, some objectionable material exists. The Board will provide pupil access to Internet resources only in supervised environments and has taken steps to lock out objectionable areas to the extent possible, but potential dangers remain. 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 the system administrators 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 accounts on the system should be aware of the existence of such materials and monitor home usage of the school district computer network. 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 pupil's 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 a system administrator 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 member's account and other action in compliance with the 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.

Users and their parent(s) or legal guardian(s) specifically agree to indemnify the River Vale School District and the system administrators for any losses, costs, or damages, including reasonable attorney's fees incurred by the Board relating to, or arising out of any breach of this section by the user.

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

Software Libraries on the Network

Software libraries on the network are provided to pupils as an educational resource. No pupil may install, upload, or download software without the expressed consent of the system 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. The system administrators, at their sole discretion, reserve the rights to refuse posting of files and to remove files. The system administrators, at their sole discretion, 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 network/computers without the author's specific written permission. Only the owner(s) or persons they specifically authorize may upload copyrighted material to the system. Members may download copyrighted material for their own use in accordance with Policy and Regulation Nos. 2531, Copying Copyrighted Materials. Any member may also noncommercially 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.

Public Posting Areas (Message Boards/Usenet Groups)

Usenet messages are posted from systems connected to the Internet around the world and the school district system administrators have no control of the content of messages posted from these other systems. To best utilize system resources, the system administrators will determine which Usenet groups are most applicable to the educational needs of the school district and will carry these groups on the school district computer network. The system administrators, at their sole discretion, may remove messages posted locally that are deemed to be unacceptable or in violation of the Board policies and regulations. The system administrators, at their sole discretion, further reserve the right to immediately terminate the account of a member who misuses the message boards or Usenet groups.

Real-time, Interactive, Communication Areas

The system administrators, at their sole discretion, 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 member 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 the system are retained on the system until deleted by the recipient or for a maximum of fifteen days. A canceled account will not retain its E-mail. Members are expected to remove old messages within fifteen days or the system administrators may remove such messages. The system administrators 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 networks or computers.

Disk Usage

The system administrators reserve the right to set quotas for disk usage on the system. A member who exceeds his/her quota of disk space will be advised to delete files to return to compliance with predetermined quotas. A member who remains in noncompliance of disk space quotas after seven school days of notification will have their files removed by a system administrator.

Security

Security on any computer system is a high priority, especially when the system involves many users. If a member feels that he/she can identify a security problem on the computer network, the member must notify a system administrator. The member should not inform individuals other than the system administrators or other designated members of the school district staff of a security problem. Professional staff may allow individuals who are not members to access the system through the staff personal account as long as the staff person does not disclose the password of the account to the individuals and understands that the staff person assumes responsibility for the actions of individuals using his/her account. Members may not otherwise allow others to use their account and password. Passwords to the system should not be easily guessable by others, nor should they be words, which could be found in a dictionary. Attempts to log in to the system using either another member's account or as a system administrator will result in termination of the account. Members should immediately notify a system administrator if a password is lost or stolen, or if they have reason to believe that someone has obtained unauthorized access to their account. Any member 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 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 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. Printing for other than educational purposes is prohibited.

Internet Sites and the World Wide Web

The system administrator may establish an Internet site(s) on the World Wide Web or other Internet locations. Such sites shall be administered and supervised by the system administrator,

who shall ensure that the content of the site complies with 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 Director of Educational Technology in matters relating to the use of computer networks/computers and by the Principal in matters of school suspension. 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 are 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.

Decisions of the Director of Educational Technology may be appealed in accordance with Policy No. 5710 Pupil Grievances.