ACCEPTABLE USE POLICY (AUP)

Instruction

Overview

The Board of Education provides computer resources to support its educational objectives. Proper use of electronic information technology enhances the curriculum and learning opportunities for students as well as the teaching resources of school personnel.

The intent of this policy is to:

1. Promote the safe use of the District's computer resources by students and other users;
2. Prevent the misuse of computer resources by users.

When used in this policy, the term "computer resources" refers to the school's entire computer network. This includes, the school's computer system, file servers, database servers, application servers, communication servers, mail servers, fax servers, web servers, work stations, stand-alone computers, Chromebooks, laptops, software, data files, and all internal and external computer and communications networks that may be accessed directly or indirectly from the school's computer network. It therefore includes all e-mail services and Internet access.

This policy applies to all users of the District's computer resources. The term "users" includes students, employees, independent contractors, consultants, temporary workers, volunteers and all other persons or entities who use or come in contact with the District's computer resources. By using or accessing the District's computer resources, users agree to abide by this policy.

Any personal electronic devices which are brought into, or connected to the information networks of the District on or off school grounds shall be subject to this policy and related regulations.

Internet Safety and Access

Electronic information research skills are now fundamental for productive citizens and employees. Access to the Internet enables students, teachers, and administrators to explore thousands of libraries, databases, bulletin boards, and other resources while exchanging information with people around the world. Unfortunately, the Internet is also a source of highly inappropriate material. In an effort to minimize student exposure to inappropriate material on the Internet, the following protective measures will be employed by the District:

1. On-line activities of all users will be monitored.

2. The District will employ a technology protection measure that protects against Internet access by both adults and minors to visual depictions that are obscene, pornographic, or, with respect to the use of computers by minors, harmful to minors as defined by the Children's Internet Protection Act. Such technology protection

measure shall be in operation during any use of computers with Internet access. However, it is recognized that this measure alone is no guarantee that users will not be able to find Internet resources which are profane, offensive, obscene, or otherwise objectionable. The ultimate responsibility for appropriate use of Internet resources lies with the user.

3. The District expects that its teachers will blend thoughtful use of the Internet throughout the curriculum and will provide guidance and instruction to students in its use. As much as possible, access from school to Internet resources should be structured in ways which point students to those which have been evaluated prior to use. Students may be able to move beyond those resources to others that support learning objectives. If necessary, school personnel may request, in writing, that the technology protection measure be disabled for use by an adult for the purpose of bona fide research or other purpose that promotes an educational objective. The ***Director of Information Technology and/or school principals*** are authorized to approve such requests.

4. Students utilizing District-provided Internet access must first have the permission of and must be supervised by the District's staff. School personnel who supervise student use of the Internet will give students instruction, as appropriate, regarding appropriate on-line behavior, including interacting with other individuals on social networking sites and in chat rooms and cyberbullying awareness and response. School personnel who supervise student use of the Internet shall limit and/or closely monitor forms of direct electronic communication, such as chat rooms and e-mail. Students utilizing school-provided Internet access are responsible for good behavior on-line just as they are in a classroom or other area of the school. To remain eligible as users, students' use must be in support of and consistent with the educational objectives of the District.

5. Access to the Internet is a privilege and not a right. It is expected that all users will act in a responsible and legal manner in accordance with District policy and state and federal laws.

<u>Security</u>

Each user is responsible for ensuring that use of outside computers and networks, such as the Internet, does not compromise the security of the District's computer resources. This duty includes taking reasonable precautions to prevent intruders from accessing the District's network without authorization.

Viruses can cause substantial damage to computer systems. Each user is responsible for taking reasonable precautions to ensure he or she does not introduce viruses into the District's network. All material not belonging to the District must be scanned for viruses prior to being placed onto the District's computer system. Users should understand that their home computers and laptops might contain viruses. All disks, memory sticks or perpetual media (e.g., DVD, CD) transferred from these computers to the District's network must be scanned for viruses.

Prohibited Activities

Users are not permitted to use school-provided computer resources to:

1. "Hack into," "snoop," monitor any network traffic or otherwise access data not intended for the user including, but not limited to, other users' files and administrative data;

2. Share passwords with others, circumvent the menu/password and/or Internet filtering software installed on District computers;

3. Create, use, access, upload, download, transmit or distribute profane, pornographic, obscene, sexually explicit, harassing, threatening or illegal material or communications;

4. Harass, cyber bully or intentionally offend others;

5. Vandalize, damage, or disable the property of another individual or organization including destroying data by creating or spreading viruses or by other means;

6. Intentionally disrupt or degrade network activity;

7. Violate copyright or otherwise use the intellectual property of another individual or organization without permission;

8. Plagiarize (to take material created by others and presenting it as if it were one's own) or cheat (to deceive by trickery, mislead or fool):

9. Send, transmit, or otherwise disseminate proprietary data, personal information about minors or other confidential information;

10. Violate any local, state, or federal law or school policy.

Users may not do any of the following without prior written authorization from the school administration:

1. Access the District networks with privately owned laptop computers, cell phones, I-pads, or any other personal electronic devices
2. Copy software for use on their home computers;
3. Provide copies of software to any independent contractors or clients of the District or to a third person;
4. Install software on any of the District's work stations or servers;
5. Download any software from the Internet or other on-line service to any of the District's work stations or servers;
6. Modify, revise, transform, recast, or adapt any software;
7. Reverse engineer, disassemble or decompile any software.

No Expectation of Privacy

All users are warned that there should be no expectation of privacy in connection with the use of the District's computer resources. Users should not create, store or use messages, files or other information which they do not want school authorities to see. The following reasons explain why users should have no expectation of privacy:

1. The District may have a duty under federal law to monitor on-line activities of users and enforce the use of protective measures. Authorized administrators and staff may review use of the District's computer resources and the Internet at any time, without reason or prior notice, to maintain system integrity and determine that users are acting responsibly or otherwise consistent with this policy.

2. Computer resources are owned, controlled, and maintained by the District. They are provided to staff and students to be used for educational purposes only. Files or any information stored on school-based networks are subject to periodic inspection and routine maintenance.

3. E-mail communications can be stored indefinitely on any number of computers. Copies of messages may be forwarded to others either electronically or on paper. In addition, e-mail sent to non-existent or incorrect user names may be delivered to persons that you never intended.

4. Use of passwords to gain access to the computer network or to encode particular files or messages does not imply that users have an expectation of privacy in such access or materials. The District has global passwords that permit it to access all material stored on the computer system, regardless of whether that material has been encoded with a particular user's password.

5. District personnel may receive or create e-mail messages and other documents that are public records that may be subject to disclosure under the Freedom of Information Act.

Use of Computer Resources by School Personnel

The computer resources are the property of the District and may only be used for approved purposes. Users are permitted access to assist them in the performance of their jobs. Occasional use of the computer resources by an individual school employee for personal communications is permitted when the use does not interfere with the employee's or other user's job responsibilities, performance of the computer resources, or operation of the District. A short social message and a quick note to a family member are examples of permitted personal use. Use for personal or third party gain or profit, or for entertainment, is strictly prohibited. Solicitation for any purpose, other than to support a community service drive officially sponsored by the District, will not be tolerated. Employees are reminded that this limited, occasional personal use must comply with this policy, and all other policies, regulations and practices of the District. Use of computer resources is a privilege that may be revoked at any time, in whole or in part, at the sole discretion of the District.

Policy Violations

Users who become aware of any misuse of computer resources must immediately report the incident to the administration. Any violation of this policy may result in immediate termination of school-provided access to computer resources, including the Internet. Additional disciplinary action may be taken in keeping with existing policies, procedures and practices regarding the conduct, including but not limited to suspension and/or expulsion from school (students) or termination of employment (personnel). When appropriate, law enforcement agencies may be involved and legal action or prosecution may result.

Limitations

The Board makes no warranties of any kind, neither expressed nor implied, for the use of computer resources and the Internet access it is providing. The District will not be responsible for any damages users suffer, including--but not limited to--loss of data resulting from delays or interruptions in service; the accuracy, nature, or quality of information stored on District diskettes, hard drives, or servers; the accuracy, nature, or quality of information gathered through District-provided Internet access; personal property used to access District computers or networks or for school-provided Internet access; nor for unauthorized financial obligations resulting from school-provided access to its computer resources and the Internet.

Notice of Policy

Students and school personnel shall be given notice of this policy annually. All other users shall be given notice of this policy prior to obtaining access to or using District computer resources.

Each user is required to sign an Acknowledgement Form stating that they have received notice of and understand this policy and any accompanying administrative regulations.

The administration may issue regulations in connection with this policy.

Legal References:

20 U.S.C. 6777 Internet Safety (Children's Internet Protection Act)
47 U.S.C. 254 Universal Service
45 C.F.R. 54.520, "Children's Internet Protection Act certifications required from recipients of discounts under the federal universal service support mechanism for schools and libraries";

Policy approved: 12/11/2001
Policy revised: 11/11/2021

Appendix A

Acceptable Use Agreement

Internet access is available to students and staff in the Regional School District No. 7 schools. The Board of Education believes the Internet offers vast, diverse and unique resources to both students and staff. To the greatest extent possible, the Board seeks to filter out objectionable services on the Internet. Total elimination of access to objectionable content is not possible. Individual student users must take responsibility for their own activities when navigating the Internet. Anyone with security/technical violations or who inadvertently accesses objectionable materials should report this immediately to the staff member in charge. Our goal in providing this service to staff and students is to promote educational excellence in the schools by facilitating resource sharing, innovation, and communication.

Student

I understand and will abide by the Regional School District No. 7 Acceptable Use Agreement Policy and the corresponding procedures and guidelines. I understand that this access is designed for educational purposes. I further understand that any violation of the policy or corresponding procedures and guidelines is unethical and may constitute a criminal offense. Should I commit any violation, of said policy or corresponding procedures and guidelines, my access privileges may be revoked, and school disciplinary action as deemed appropriate by the administration and/or appropriate legal action may be taken.

Name of student_____

Signature of Student_____ Date_____

School _____ Grade_____

Parent or Guardian (Student under age 18)

As the parent or guardian of this student, I have read the Acceptable Use Policy. I understand that this access is designed for educational purposes. I also recognize it is impossible for Regional School District No. 7 to restrict access to all controversial materials and I will not hold the school system responsible for materials students may acquire on the network. I hereby give permission for my child to access the Internet, be issued an account if necessary and also certify that the information on this form is correct. I understand that any violation of the schools' policy, procedures and guidelines by my child may result in loss of access privileges, disciplinary action as deemed appropriate by the administration and/or appropriate legal action may be taken.

Name of Parent or Guardian _____
(Please print)

Signature of Parent or Guardian_____ Date_____

Appendix B

EMPLOYEE ACKNOWLEDGMENT

REGARDING

COMPUTER AND INTERNET USE

I have read and agree to comply with the terms of the Regional School District No. 7 Board of Education's policy # 6141 and accompanying regulations governing the use of the District's computer resources by school personnel. I understand that a violation may result in disciplinary action, including possible termination, as well as civil or criminal liability. I also understand that I am responsible for financial obligations resulting from my unauthorized use of the computer resources, and that the District may revoke my access privileges at any time.

Signature: _____ Date: _____

Print: _____

Appendix C

NOTICE REGARDING ELECTRONIC MONITORING
of School District Personnel

In accordance with Connecticut law, Regional School District No. 7 ("District") hereby gives notice to all its employees of the potential use of electronic monitoring in its workplace. While the District may not actually engage in the use of electronic monitoring, it reserves the right to do so as management deems appropriate in its discretion, consistent with the provisions set forth in this notice.

"Electronic monitoring", means the collection of information on District premises concerning employees' activities or communications, by any means other than direct observation of the employees. Electronic monitoring includes the use of a computer, telephone, wire, radio, camera, electromagnetic, photo electronic or photo-optical systems.

The law does not cover the collection of information for security purposes in any common areas of District premises which are open to the public, or which is prohibited under other state or federal law.

The following specific types of electronic monitoring may be used by the District in its workplaces:

- Monitoring of e-mail, Internet usage and other components of the District's computer resources for compliance with its policies, procedures and guidelines concerning use of such resources.

- Video and/or audio surveillance within the District's facilities (other than in restrooms, locker rooms, lounges and other areas designed for the health or personal comfort of employees or for the safeguarding of their possessions).

- Monitoring of employee usage of District's telephone systems.

The law also provides that, where electronic monitoring may produce evidence of misconduct, the District may use electronic monitoring without any prior notice when it has reasonable grounds to believe employees are engaged in conduct that violates the law, violates the legal rights of the District or other employees, or creates a hostile work environment.