

Instruction

Internet/Computer Networks Use

The Internet and electronic communications (e-mail, chat rooms and other forms of electronic communication) have vast potential to support curriculum and student learning. The Council believes they should be used in schools as a learning resource.

Use of the Internet and electronic communications requires students to think critically, analyze information, write clearly, use problem-solving skills, and hone computer and research skills that employers demand. Use of these tools also encourages an attitude of lifelong learning and offers an opportunity for students to participate in distance learning activities, ask questions of and consult with experts, communicate with other students and individuals, and locate material to meet educational and personal information needs.

The Council believes the educational opportunities inherent in these tools far outweigh the possibility that users may procure material not consistent with the education goals of CREC. However, the Internet and electronic communications are fluid environments in which students may access materials and information from many sources, including some that may be harmful to them. CREC acknowledges that while it is impossible to predict with certainty what information students might locate or come into contact with, it shall take all reasonable steps to protect students from accessing material and information that is obscene, pornographic or otherwise harmful to minors, as defined by CREC. Students shall take responsibility for their own use of CREC's computers and computer systems to avoid contact with material or information that may be harmful to minors.

Guidelines for General Use

1. All use of the Internet, electronic services, or any telecommunications network must be in support of educational objectives or research.
2. Any electronic mail accounts shall be used only by the authorized owner of the account. Account owners are ultimately responsible for all activity under their account.
3. Any use of CREC's computing resources or networks for illegal or inappropriate purposes, any accessing of materials that are inappropriate in a public school environment, or any acts supporting such activities, is prohibited.
5. Any use of telecommunication opportunities for commercial purposes, financial gain, product advertisement, political lobbying, or attempt to disrupt the use of the services by others, is prohibited.

Blocking or Filtering Obscene, Pornographic and Harmful Information

Software blocks or filters material and information that is obscene, pornographic or otherwise harmful to minors, as defined by the Council, from reaching all CREC computers having Internet or electronic pornographic, harmful to minors, or otherwise in violation of this policy to their teacher. Students communications access. Students shall report access to any material and information that is obscene,

who become aware of other students accessing such material or information, shall report it to their teacher.

No Expectation of Privacy

CREC computers and computer systems are owned by CREC and are intended for educational purposes at all times. Students shall have no expectation of privacy when using the Internet or electronic communications. CREC reserves the right to monitor, inspect, copy, review, and store (at any time and without prior notice) all usage of CREC computers and computer systems, including all Internet and electronic communications, access and transmission/receipt of materials and information. All material and information accessed/received through CREC computers and computer systems shall remain the property of CREC.

Unauthorized and Unacceptable Users

Students shall use CREC computers and computer systems in a responsible, efficient, ethical and legal manner.

Examples of unacceptable uses include, but are not limited to,:

Intentionally accessing, creating, transmitting, retransmitting, or forwarding material or information that:

- Promotes violence or advocates destruction of property including, but not limited to, information concerning the manufacturing or purchasing of destructive devices or weapons;
- Is not related to CREC education objectives;
- Contains pornographic, obscene or other sexually oriented materials, either as pictures or writings that are intended to stimulate erotic feelings or appeal to prurient interests;
- Harasses, threatens, demeans, or promotes violence or hatred against another person or group of persons on the basis of their race, color, sex, religion, national origin, age, marital status, disability or handicap;
- Is for personal profit, financial gain, advertising, commercial transaction, or political purposes;
- Plagiarizes the work of another;
- Uses inappropriate or profane language that is offensive in the school community;
- Is knowingly false or intended to damage another person's reputation;
- Is in violation of any federal or state law, including but not limited to, copyright and trade mark protections;
- Contains private information about oneself or others, including information protected by confidentiality laws;
- Uses another individual's Internet or electronic communications account without permission from that individual;
- Impersonates another or transmits through an anonymous remailer; and
- Accesses fee services without specific permission from the system administrator.

Security

Security on CREC computer systems is a high priority. Students who identify a security problem while using the Internet or electronic communications must immediately notify their teacher, who will then notify the system administrator. Students shall not demonstrate the problem to other users. Logging on to the Internet or electronic communications as a system administrator is prohibited.

Students shall not:

- use another person's password or any other identifier;
- gain or attempt to gain unauthorized access to CREC computers or computer systems; or
- read, alter, delete, copy, or attempt to do so, electronic communications of other system users.

Any user identified as a security risk, or as having a history of problems with other computer systems, may be denied access to the Internet and electronic communications.

Safety

Students shall not reveal personal information, such as home address or phone number, while using the Internet or electronic communications. Without first obtaining permission of their teacher, students shall not use their last name or any other information that might allow another person to locate them. Students shall not arrange face-to-face meetings with persons met on the Internet or through electronic communication.

Vandalism

Vandalism will result in cancellation of privileges and may result in school disciplinary action and/or legal action. Vandalism is defined as any malicious or intentional attempt to harm, destroy, modify, abuse, or disrupt the operation of any network within CREC, any network connected to the Internet, operation of electronic communications, the data contained on any network or electronic communications, the data of another user, usage by another user, or CREC-owned software or hardware. This includes, but is not limited to, the uploading or creation of computer viruses and the use of encryption software.

Unauthorized Software

Students are prohibited from using or possessing any software that has not been authorized by CREC.

Assigning Student Projects and Monitoring Student Use

CREC will make every effort to see that the Internet and electronic communications are used responsibly by students. Administrators, teachers, and staff have a professional responsibility to work together to monitor students' use of the Internet and electronic communications, and to help students develop the intellectual skills needed to discriminate among information sources, identify information appropriate to their age and developmental levels, and evaluate and use information to meet their educational goals. Students shall have specifically defined objectives and search strategies prior to

accessing material and information on the Internet and through electronic communications.

All students shall be supervised by staff while using the Internet or electronic communications.

Student Use is a Privilege

Use of the Internet and electronic communications demands personal responsibility and an understanding of the acceptable and unacceptable uses of such tools. Student use of the Internet and electronic communications is a privilege, not a right. Failure to follow the use guidelines contained in this policy will result in the loss of the privilege to use these tools and may result in school disciplinary action and/or legal action. CREC may deny, revoke, suspend access to CREC technology, close accounts, or take other appropriate action at any time.

Students and parents/guardians shall be required to sign the CREC Acceptable Use Agreement annually before Internet or electronic communication accounts shall be issued or access is allowed.

CREC Makes No Warranties

CREC makes no warranties of any kind, whether expressed or implied, related to the use of CREC computers and computer systems, including access to the Internet and electronic communications services. Providing access to these services does not imply endorsement by CREC of the content, nor does CREC make any guarantee as to the accuracy or quality of information received. CREC shall not be responsible for any damages, losses or costs a student suffers in using the Internet and electronic communications. This includes loss of data and service interruptions. Use of any information obtained via the Internet and electronic communications is at the students' own risk.

Legal Reference: Connecticut General Statutes

53a-182b. Harassment in the first degree: Class D felony.

53a-183. Harassment in the second degree: Class C misdemeanor

Other

20 U.S.C. Sections 6777, No Child Left Behind Act

20 U.S.C. 254 Children's Internet Protection Act of 2000

47 U.S.C. Children's Online Protection Act of 1998

Policy adopted: January 21, 2009

Revised: April 17, 2024

CAPITOL REGION EDUCATION COUNCIL

Hartford, Connecticut