

ESU 10 AND LITCHFIELD SCHOOLS ACCEPTABLE USE POLICY

Litchfield Public Schools Internet Safety Policy -- 5131.8

TECHNOLOGY/INTERNET SAFETY POLICY

It is the policy of Educational Service Unit 10 that access to the Internet provided by ESU 10 is expected to be used as an educational and/or work-related resource and that such access shall be made available subject to such rules and regulations as may be established, provided that no use shall be permitted which, in the judgment of the Board of Directors of ESU 10, is in any way prejudicial to the best interest of the unit or in conflict with the ESU 10 Program of Services.

The ESU 10 Board of Directors and Litchfield Public Schools reserves the right to refuse access to the Internet by ESU 10 to anyone when it deems it necessary in the public interest.

Definitions

1. Access to the Internet—A computer shall be considered to have access to the Internet if such computer is equipped with a modem or is connected to a computer network which has access to the Internet.
 - a. At school, the only allowable connection is through the wireless network “**LPS WLAN**”
2. Minor shall mean an individual who has not attained the age of 19.
3. Obscene shall have the meaning given such term in section 1460 of title 18, United States Code.
4. Child pornography shall have the meaning given such term in section 2256 of title 18, United States Code.
5. Harmful to minors shall mean any picture, image, graphic image file, or other visual depiction that:
 - a. taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;
 - b. depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and
 - c. taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.
6. Hacking shall mean attempting to gain unauthorized access to computer and network systems both standalone and connected to the Internet.
7. Technology protection measure shall refer to a proxy server managed by ESU 10 that blocks and/or filters Internet access or other means by which access may be blocked and/or filtered.
8. Authorized staff member as used herein shall refer to an adult staff member appointed by the Litchfield Public Schools Technology Committee.
9. Technology Committee as used herein shall refer to a group of Litchfield Public Schools staff members.

ACCESS TO TECHNOLOGY/INTERNET BY MINORS

Minors accessing Technology/Internet services provided by Litchfield Public Schools shall be subject to the following rules and regulations:

1. Minors shall not access material that is obscene, child pornography, harmful to minors, or otherwise inappropriate for educational.
2. Minors shall not use Litchfield Public Schools technology or Internet resources to engage in hacking or attempts to otherwise compromise any computer or network system's security.
3. Minors shall not engage in any illegal activities on Technology/Internet.
4. Minors should only use electronic mail, chat rooms, and other forms of direct electronic communications for purposes related to education within the context of a school-related assignment activity.
5. Minors shall not disclose personal identification information on the Internet.

Access to Technology/Internet by Adults

Adults accessing Technology/Internet services provided by Litchfield Public Schools shall be subject to the following rules and regulations:

1. Adults shall not access material that is obscene, child pornography, or otherwise inappropriate for training or work-related uses.
2. Adults shall not use Litchfield Public Schools technology resources to engage in unauthorized hacking or attempts to otherwise compromise any computer or network system's security.
3. Adults shall not engage in illegal activities on Technology/Internet.

Technology Protection Measure

Litchfield Public Schools shall use a technology protection measure that blocks and/or filters Internet access to prevent access to Internet sites that are not in accordance with the policies of Litchfield Public Schools.

1. The technology protection measure that blocks and/or filters Internet access may be disabled by an authorized staff member for bona fide research purposes with permission of the immediate supervisor of the staff member requesting said disabling or with the permission of the administrator of Litchfield Public Schools.
2. An authorized staff member may override the technology protection measure that blocks and/or filters Internet access for a minor to access a site for bona fide research or other lawful purposes during which time the minor will be monitored directly by the authorized staff member or his/her designee.

Policy Violations

Any violation of this policy may result in the loss of access to the Internet by Litchfield Public Schools and/or ESU 10. Additional disciplinary action may be determined in accordance with existing procedures and practices, both administrative and as stipulated in Litchfield Public Schools and/or ESU 10 board policy, and including applicable law enforcement agencies when necessary.

POLICY ADOPTED: 2016

LITCHFIELD PUBLIC SCHOOL

REVISED:

LITCHFIELD, NE 68852

REVISED:

ACCEPTABLE USE OF COMPUTERS, TECHNOLOGY AND THE INTERNET

Due to the rapidly changing nature of technology, most specific rules in this area are best left to coverage under administrative regulations that will be developed by the administration.

The Board supports the use of computers, technology and the Internet in the District's instructional program as a resource to educate and inform. The use of these resources shall be consistent with the curriculum adopted by the School District and shall be employed in an appropriate and responsible manner to meet the varied instructional needs, learning styles, abilities and developmental levels of students.

Technology resources of the district shall not be used for personal use unless the user has entered into an agreement with the district that makes such use compliant with the law.

PROCEDURES AND GUIDELINES

The Superintendent shall develop and implement appropriate procedures to provide guidance for computer use and Internet access. Guidelines shall address teacher supervision of computer use, ethical use of electronic media, and the District's ownership and right of administrative review of electronic files and communications. The term "electronic media" includes, but is not limited to, the Internet, e-mail and other technological resources.

The guidelines shall prohibit utilization of networks for inappropriate or illegal activities, the intentional spreading of embedded messages (viruses) or the use of other programs with the potential of damaging or destroying programs, data or equipment. The guidelines will describe the District's limitation of liability and will establish that the use of computers, technology and the Internet is a privilege, not a right. Violation of the procedures and guidelines will result in cancellation of those privileges and appropriate disciplinary action.

Technology Protection Measure

The District will implement a technology protection measure that will block or filter Internet access to visual depictions that are obscene, pornographic or of a harmful nature to minors. Operation of this measure will be monitored and enforced during use of computers by minors.

Audit of Use

Users with network access shall not utilize District resources to establish electronic mail accounts through third-party providers or any other nonstandard electronic mail system. Participation in chat rooms is prohibited without specific prior approval by the system administrator. The Superintendent shall establish a process to determine whether the District's education technology is being used for purposes prohibited by law or for accessing prohibited materials. The process may include, but not be limited to:

1. Utilizing blocking/filtering software.
2. Turning off the "auto load images" feature of the Internet browser.
3. Using a proxy server to control accessible websites.

Appropriate Internet Behavior On Social Websites

The district recognizes its responsibility to educate students regarding appropriate behavior on social networking and chat room sites about cyber-bullying. Therefore, students shall be provided instruction about appropriate online behavior, including interacting with other individuals on social networking sites and in chat rooms and cyber-bullying awareness and response. The district will create an age-appropriate plan for providing such instruction using informational programs, educational materials and lessons as needed to achieve this goal.

STUDENT USE

A written parental permission and agreement form will be required prior to the student being granted access to electronic media involving District technological resources. The form will specify acceptable uses, rules of on-line behavior, access privileges and penalties for procedural violations. It must be signed by the parent or legal guardian of minor students (under age 18) and by the student. This document will be kept on file as a legal, binding document. In order to rescind the agreement, the student's parent/guardian (or the student who is at least 18 years old) must provide the Superintendent with a written request.

The district will obtain verifiable parental consent prior to allowing third parties to collect personal information online from students in compliance with the Children's Online Privacy Protection Act.

STAFF USE

A written staff agreement form will be required for all employees having access to electronic media. Staff shall confine e-mail use to work-related purposes and a reasonable, appropriate and limited personal use that does not interfere with their district duties. The agreement form will refer to the procedures and guidelines for use of computers and the Internet, describe prohibitions and limitations on the use of these resources and state the employee's responsibility for the security of individual passwords.

COMMUNITY USE

On recommendation of the Superintendent, the Board will determine the conditions and limits under which equipment and services will be made available to the community. Upon request to the Building Principal, community members may have access to electronic resources and programs available through the District, provided they attend any required training and abide by the rules of usage established by the Superintendent. A written agreement form will be required for all community members having access to these resources indemnifying the District from claims by community users.

DISREGARD OF RULES

Individuals who refuse to sign required acceptable use documents or who violate District rules governing the use of District technology shall be subject to loss or restriction of the privilege of using computers, technology or the Internet and related resources.

RESPONSIBILITY FOR DAMAGES

Individuals shall reimburse the Board for repair or replacement of District property lost, stolen, damaged, or vandalized while under their care.

RESPONDING TO CONCERNS

School officials shall apply the same criterion of educational suitability used to review other educational resources when questions arise concerning access to specific databases or other electronic media.

Legal Reference: 20 U.S.C. sec. 1232g (1988) (Family Educational Rights and Privacy Act)
47 U.S.C. 201 et seq. (Communications Decency Act of 1995)
Children's Internet Protection Act and Neighborhood CIPA of 2000
Children's Online Privacy Protection Act of 1998 with revisions
Nebraska Statutes 79-2104

Cross Reference: 102 Educational Philosophy of the District
401 Guiding Principles for Employees
504 Student Rights and Responsibilities
507 Student Records
603 Curriculum Development
604 Instructional Curriculum
1006 Use of District Facilities and Equipment