

#### SERVICES TO SCHOOLS AND CHILDREN

### Section 8 Use of Building & Property

## A. Weapons

The Board of ESU #13 believes weapons and other dangerous objects and look-a-likes in ESU #13 facilities can cause material and substantial disruption to the ESU #13 environment or present a threat to the health and safety of students, employees and visitors on ESU #13 premises or property within the jurisdiction of the ESU #13.

Weapons and other dangerous objects and look-a-likes shall be taken from students and others who bring them onto the ESU #13 property or onto property within the jurisdiction of ESU #13 or from students who are within the control of the ESU #13. For purposes of this policy, the term "dangerous object" includes any personal safety or security device (such as tasers, mace and pepper spray). This prohibition includes persons with a permit to carry a concealed handgun. Possession of a weapon includes, without limitation, a weapon in a person's personal possession or control, including a weapon in a desk, locker, backpack or purse. A person who is uncertain as to what constitutes a "dangerous object" under this policy is strongly encouraged to contact the Program Administrator or the Program Director in advance of such person bringing the item onto ESU #13 property. Any person found to be in violation of this policy shall be subject to disciplinary action, up to and including termination.

Parents of students found to possess weapons or dangerous objects or look-a-likes on ESU #13 property shall be notified of the incident. Confiscation of weapons or dangerous objects shall be reported to the law enforcement officials, and students will be subject to disciplinary action including suspension or expulsion.

Students bringing firearms to ESU #13 or knowingly possessing firearms at the ESU #13 may be expelled for a period of not less than one year. Students bringing to ESU #13 or possessing dangerous weapons, including firearms, will be referred to law enforcement authorities. The Program Administrator or Program Director shall have the authority to recommend this expulsion requirement be modified for students on a case-by-case basis.

Weapons under the control of law enforcement officials shall be exempt from this policy. Firearms also may be possessed by a person for the purpose of using them, with the approval of ESU #13, in a historical reenactment, in a hunter education program, or as part of an honor guard. The Program Administrator or Program Director may allow authorized persons to display weapons or other dangerous objects or look-a-likes for educational purposes. Such a display shall also be exempt from this policy.

Legal Reference:	
Date of Adoption:	December 15, 2020
Updated:	

### B. Use of Metal Detectors

When ESU #13 administration has reasonable cause to believe that weapons are in the possession of unidentified students, when there has been a pattern of weapons found at ESU #13 or when violence involving weapons has occurred at ESU #13 or at ESU #13 sponsored events, the administration shall be authorized to use stationary or mobile metal detectors in accordance with procedures approved by the Board.

Any search of a student's person as a result of the activation of the detector shall be conducted in private in accordance with the policy on Searches, Seizures and Arrests.

Legal Reference:	
Date of Adoption:	December 15, 2020
Updated:	

# C. Security

The Board of ESU #13 encourages cooperation with the local law enforcement and the fire authorities and insurance company personnel in planning and carrying out proper security measures to preserve and protect ESU #13's investment in its physical plant. Buildings constitute one of the greatest capital investments of ESU #13 and should be protected. Security includes minimizing fire or other safety hazards, reducing the probability of faulty equipment, and keeping records and funds in a safe place. Security also includes having available floor plans of buildings and site plans showing the boundaries and access points.

A key control system shall be established and maintained limiting building access to ESU #13 personnel thus safeguarding against potential entry by unauthorized persons.

Protective devices designed as safeguards against illegal entry and vandalism shall be installed where appropriate. A security guard may be employed when special events or activities are scheduled, or in situations involving special risks.

The Program Administrator or Program Director is directed to establish regulations as may be needed to provide for security of building and grounds.

Incidents of illegal entry, theft of school property, vandalism or damage to ESU #13 property from any cause shall be reported by phone to the office of the Program Administrator or Program Director and to the appropriate law enforcement agency as soon as discovered. A timely written report of the incident shall be forwarded to the Program Administrator or Program Director.

ESU #13 will share the levels of protection with local fire departments, law enforcement and 911 communications to include location of the Knox Box and other safeguards and contact information for after-hour emergencies on ESU #13 properties.

Legal Reference:	
Date of Adoption:	December 15, 2020

### D. Access to Buildings

Security for ESU #13 buildings and grounds (at all times) contributes to the well-being and safety of its students and staff as well as to that of the sites themselves.

The Program Administrator or Program Director will control access to the ESU #13 buildings and other facilities as appropriate and necessary to protect property, students and personnel.

Card access to buildings is determined and controlled through the issuances of key cards. Hours shall be determined and enforced by the Program Administrator or the Program Director.

The Program Administrator or Program Director will control access to the ESU #13 buildings and will provide safeguards against unauthorized access to these buildings. Each Program Administrator or Program Director, with the ESU #13 Administrator's approval, will develop regulations designed to control the use of the building keys and to ensure that buildings are adequately closed and locked when no authorized personnel are present. Staff or students who fail to obey such regulations may be disciplined, suspended or dismissed.

During regular school hours, flow of traffic into and out of buildings shall be closely monitored and limited to certain doors. Visitors shall be required to check in to show proper identification and reason for being at the school and shall wear name tags identifying them as visitors. This will not apply when parents/guardians have been invited to a classroom or assembly program.

Access to school buildings outside of regular school hours shall be limited to personnel whose work requires it and to sponsors of approved student activities.

Legal Reference:	
Date of Adoption:	December 15, 2020
Updated:	

#### E. Service Animals

Individuals with disabilities, including but not limited to students, may use a service animal on ESU #13 property subject to the conditions in this policy.

#### 1. Definition

A service animal is any dog that is individually trained to do work or perform tasks for the benefit of an individual with a disability, including a physical, sensory, psychiatric, intellectual, or other mental disability. Other species of animals, whether wild or domestic, trained or untrained, are not considered service animals.

The work or tasks performed by a service animal must be directly related to the individual's disability. Examples of work or tasks include, but are not limited to:

- assisting individuals who are blind or have low vision with navigation and other tasks;
- alerting individuals who are deaf or hard of hearing to the presence of people or sounds;
- providing non-violent protection or rescue work;
- pulling a wheelchair;
- assisting an individual during a seizure;
- alerting individuals to the presence of allergens;
- retrieving items such as medicine or the telephone;
- providing physical support and assistance with balance and stability to individuals with mobility disabilities;
- helping individuals with psychiatric and neurological disabilities by preventing or interrupting impulsive or destructive behaviors.

The crime deterrent effects of an animal's presence and the provision of emotional support, well-being, comfort, or companionship are not considered work or tasks under the definition of a service animal.

#### 2. When and Where a Service Animal is Allowed Access

Individuals with disabilities can bring their service animals in to all areas of ESU #13 where members of the public, program participants, clients, customers, patrons, or invitees are allowed. A service animal can be excluded from a facility if its presence interferes with legitimate safety requirements of the facility.

ESU #13 will ask an individual with a disability to remove a service animal if the animal is not housebroken or is out of control and the individual is not able to control it. A service animal must have a harness, leash or other tether, unless the handler is unable to use a tether because of a disability or the use of a tether would interfere with the service animal's ability to safely perform its work or tasks. In these cases, the service animal must be under the handler's control through voice commands, hand signals, or other effective means. If a service animal is excluded, the individual with a disability must still be offered the opportunity to obtain goods, services, and accommodations without having the service animal on the premises.

# 3. Asking Questions

To determine if an animal is a service animal, ESU #13 may ask two questions:

- a. Is this animal required because of a disability?
- b. What work or task has this animal been trained to perform?

These questions may not be asked if the need for the service animal is obvious (e.g.,

the dog is guiding an individual who is blind or is pulling a person's wheelchair). ESU #13 may not ask about the nature or extent of an individual's disability or require documentation, such as proof that the animal has been certified, trained or licensed as a service animal, or require the animal to wear an identifying vest.

### **Service Animals Other Than Dogs**

ESU #13 can consider whether the facility can accommodate service animals other than dogs, and will review requests on an individual basis. The animal must have been individually trained to do work or perform tasks for the benefit of the individual with a disability. The rules that apply to service dogs also apply to other animals.

#### **Other Provisions**

- 1. ESU #13 is not responsible for the care and supervision of a service animal.
- 2. ESU #13 cannot ask nor require an individual with a disability to pay a surcharge or deposit, even if people accompanied by pets are required to pay such fees.
- 3. If ESU #13 normally charges individuals for the damage they cause, an individual with a disability may be charged for damage caused by his or her service animal.

Legal Reference:	
Date of Adoption:	December 15, 2020
Updated:	

### F. Video Surveillance Policy

#### 1. Purpose

The ESU #13 Board authorizes the use of video cameras and other passive electronic measures (such as motion detectors) for the purposes of ensuring the health, welfare and safety of staff, students and visitors, safeguarding ESU #13 facilities and equipment, and maintaining student discipline and an appropriate educational and work environment.

#### 2. Placement

Video cameras and similar devices are authorized to be used in Unit facilities, Unit vehicles, and other places within the control of ESU #13. The locations in which the devices will be placed and the times the devices will be in use are to be determined by the Program Administrator, Program Director, or the ESU #13 Administrator or designee consistent with the purposes set forth in the Policy. The devices shall not be placed or operational in locations in which individuals have a high expectation of privacy, such as restrooms.

#### 3. Notice

Notice of the fact that video surveillance cameras are being utilized shall be given through appropriate mechanisms, such as by posting signs in the building entry and other locations and by including a notice in the student-parent and employee handbooks.

# 4. Viewing Monitors and Video Recordings

Monitors used to view video recordings are to be located and positioned such that only authorized personnel are able to see the images on the monitors. Only authorized personnel shall be allowed to view recorded video. Authorized personnel for these purposes are the Program Administrator, Program Director, the ESU #13 Administrator or designee, and the ESU #13 Technology Department personnel responsible for the technical operations of the system (for technical purposes only). In some limited circumstances, the Program Administrator, Program Director, or the ESU #13 Administrator or designee may authorize supervised viewing of surveillance cameras and recorded video by other designated staff members.

The Program Administrator, Program Director, and the ESU #13 Administrator or designee may allow law enforcement officers to view monitors and recorded video when such is consistent with school security and discipline and consistent with law.

Students shall not be permitted to view the monitors. Students shall not be permitted to view recorded video except where the individual student is the focus of the recorded video.

### 5. Use of Video Recordings

Video records may be used as a basis for student or employee disciplinary action and for making reports to law enforcement.

### 6. Video Recordings as Education Records

Video recordings which are considered to be "education records" within the scope of the Family Educational Rights and Privacy Act (FERPA) shall be maintained in accordance with FERPA and other applicable laws. A video recording may be considered an education record when a specific student is the focus of the video recording.

For example, if the video recording shows a student violating a school rule, the video recording is an education record of that student. It may be viewed on request by that student's parent (or the student if age 18 or older). The video recording

may not be viewed by, nor will a copy be given to, others without the parent's written consent unless a FERPA exception exists.

In the event more than one student is a focal point of the video recording, it may be an education record of each such student. This would be the case, for example, if two students are recorded fighting. In that event, the school would allow both sets of parents an opportunity on request to view the video, but will not give a copy of the video to either set of parents without the written consent of the other student's parent.

## 7. Maintaining Video Recordings

Video recordings shall be retained for 30 days or until determined that no incident has occurred. If an incident has been recorded, the recording will be transferred and retained concurrently with the incident file. Video recordings that contain personal information shall be securely stored in the ESU #13 network data center and, when such recordings are no longer needed or required to be maintained, shall be properly disposed of or erased.

## 8. Maintaining the Integrity of the Video Surveillance System

The ESU #13 Technology Department shall be responsible for checking the video surveillance system on a weekly basis to ensure it is operating properly. Students or staff who vandalize, damage, disable, or render inoperable surveillance cameras or equipment, or use the video surveillance system in a manner that is not consistent with the purposes set forth in this Policy, shall be subject to appropriate disciplinary action (up to and including expulsion for a student and termination for a staff member) and referral to appropriate law enforcement authorities.

Legal Reference:	
Date of Adoption:	December 15, 2020
Updated:	

## G. Internet/E-mail Acceptable Use – Student

The following are guidelines for acceptable use of the internet/e-mail:

- 1. The intent of the legislature is to provide educators and students with access on the internet/e-mail for professional growth opportunities, research, and other educationally related experiences. ESU #13 recognizes some personal use of the internet/e-mail is appropriate, being mindful any excessive personal use limits access availability for others.
- 2. Transmission or reception of any material which is in violation of any federal or state regulation is prohibited. This includes, but is not limited to: copyrighted

- material; threatening, harassing, pornographic, or obscene material; or materials protected by trade secret.
- 3. Commercial activities, product advertising, political lobbying is prohibited. Excessive personal use during the school day will be considered misuse.
- 4. Users of internet/e-mail are expected to abide by established rules of network etiquette including, but not limited to the following:
  - a. Politeness is a must at all times. Abusive messages, hate mail, harassment, discriminatory remarks, and other anti-social behaviors are prohibited.
  - b. Profanity, vulgarities, or any other inappropriate language is prohibited.
  - c. Personal phone numbers and home addresses are not to be divulged.
  - d. Network storage areas will be regarded as school property. Files and communications may be reviewed by ESU #13 personnel. Electronic mail is not guaranteed to be private.
  - e. "Chain letters" are considered to be a misuse of the system.
  - f. Talk, write, and chat commands may be intrusive and should only be used after receiving permission from the other party. Personal information should not be given.
  - g. Classroom use will take precedence over individual use.
- 5. Users must respect the integrity of the system at all times. Students and staff should not intentionally develop or activate programs that harass other users, infiltrate a computer system, or alter the software components of a computer or computer system. These include, but are not limited to: viruses, forging e-mail, hacking, and attempting to use administrative commands.
- 6. Do not vandalize or destroy the data or hardware on any other system.
- 7. Security of any computer system is essential. Access to internet/e-mail is intended for exclusive use by authorized individuals. Any problems which arise from the use of an account are the responsibility of the account holder. Misuse may result in the suspension of account privileges. This may include, but is not limited to the following:
  - a. trespassing in another's work or files
  - b. giving out your password or the password of others
  - c. attempting to login to another individual's account
  - d. failure to notify the supervising staff members of a security problem
- 8. Technology-Related Limitations: Technology resources shall not be used in any manner which impairs its effective operations or the rights of other technology users. Without limitation:

- a. Users shall not use another person's name, log-on, password, or files for any reason, or allow another to use their password (except for authorized staff members).
- b. Users shall not erase, remake, or make unusable another person's computer, information, files, programs or disks.
- c. Users shall not access resources not specifically granted to the user or engage in electronic trespassing.
- d. Users shall not engage in "hacking" to gain unauthorized access to the operating system software or unauthorized access to the system of other users.
- e. Users shall not copy, change, or transfer any software without permission from the network administrators.
- f. Users shall not write, produce, generate, copy, propagate, or attempt to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of any computer's memory, file system, or software. Such software is often called a bug, virus, worm, Trojan horse, or similar name.
- g. Users shall not engage in any form of vandalism of the technology resources.
- h. Users shall follow the generally accepted rules of network etiquette. The ESU #13 Administrator or designee may further define such rules.

Legal Reference:	47 U.S. Code § 254(h)(1)(b); 47 CFR 54.500(b) and 68 FR 36932 (2003) (E-rate restrictions)  Nebraska Statute: 49-14,101.01 (Political Accountability and Disclosure Act)  Children's Online Privacy Protection Act, 15 U.S. Code § 6501
Date of Adoption:	December 15, 2020
Updated:	