PERSONNEL

Section 7 Employee Files and Privacy

A. Employee Files

The administration shall protect the confidentiality of personal information in records regarding personnel beyond salaries and defined directory-level information. Job application materials submitted by applicants, other than finalists, who have applied for employment, shall also be maintained as confidential records. Such confidential records information shall be released only to the extent required by law or as appropriate for the operations of ESU #13.

The following information is designated as "defined directory-level information" and may be given to parents or guardians of students served by ESU #13 upon request:

1. Whether a certificated staff member has met State qualifications and licensing criteria for the grade levels and subject areas in which the certificated staff member provides instruction.

2. Whether the certificated staff member is teaching under an emergency or provisional teaching certificate.

3. The bachelor's degree major of the certificated staff member, along with information about other graduate certification or degrees held by the certificated staff member, and the field of discipline of the certification or degree.

4. The qualifications of a para-educator assigned to their child.

Information pertaining to certificated staff is also available online on the Nebraska Department of Education-Teacher Certification website.

Information regarding an employee's medical condition or history is to be maintained in a separate medical file and treated as confidential, including employment background checks related to physical or mental condition and records pertaining to FMLA leaves for health related reasons. Records maintained pursuant to the federal drug and alcohol testing laws, including drug and alcohol tests of employees and driver investigation history files for new or prospective drivers, are to be maintained in a separate file in a location with controlled access.

To the extent ESU #13 conducts any functions within the purview of the Health Insurance Portability and Accountability Act (HIPAA), which may include group health plans or student health services, it designates ESU #13 as a hybrid entity as to any such functions. The administration shall develop and implement all necessary practices and procedures to comply with laws governing protected health information (PHI) to the extent applicable and to maintain

the privacy of PHI that ESU #13 receives, obtains, or transmits. The Administrator or designee is designated as the HIPAA privacy officer for ESU #13.

Legal Reference:	Nebraska Statute: § 84-712.05 (7) and (15) (Public Records Act) 34 CFR 200.61 (NCLB) 29 CFR § 1630.14 (ADA regulations) 29 CFR § 825.500 (FMLA regulations) 49 CFR 391.23 (Drug Testing regulations) Health Insurance Portability and Accountability Act (HIPAA)
Date of Adoption: Updated:	May 19, 2020

B. Social Security Numbers

Employee social security numbers shall be kept confidential to the extent required by law. Use of more than the last four digits of an employee's social security number shall be made by ESU #13 only for:

1. Legal Mandates. Compliance with state or federal laws, rules, or regulations.

2. Internal Administration. Internal administrative purposes, including provision of employee social security numbers to third parties for such purposes as administration of personnel benefits and employment screening and staffing. However, the internal administrative uses shall not permit use of employee social security numbers:

    a. As an identification number for occupational licensing.
    b. As an identification number for drug-testing purposes except when required by state or federal law.
    c. As an identification number for ESU #13 meetings.
    d. In files with unrestricted access within ESU #13.
    e. In files accessible by any temporary employee unless the temporary employee is bonded or insured under a blanket corporate surety bond or equivalent commercial insurance.
    f. For posting any type of ESU #13 information.

3. Voluntary Transactions. Commercial transactions freely and voluntarily entered into by the employee with ESU #13 for the purchase of goods or services.

ESU #13 will not use or require an employee to use more than the last four digits of an employee's social security number for:

1. Internet Transmission. Transmission over the Internet unless the connection is secure or the information is encrypted.
2. Internet Access. To access an Internet web site unless a password, unique personal identification number, or other authentication device is also required to access the Internet web site.

3. Identifier. As an employee number for any type of employment-related activity.

Legal Reference:	Nebraska Statute: § 48-287; 5 USC § 552a (note) (Privacy Act of 1974)
Date of Adoption: Updated:	May 19, 2020

C. Shredding Consumer Reports (Background Checks)

The administration shall take reasonable measures to protect against unauthorized access to consumer information from consumer reports.[1] A consumer report includes criminal background checks performed on applicants or employees by a third party. It does not include criminal checks performed by ESU #13 staff.

Reasonable measures to protect against unauthorized access to or use of consumer information in connection with its disposal include the following examples. These examples are illustrative only and are not exclusive or exhaustive methods for complying with this directive.

1. Shredding of papers containing consumer information so that the information cannot practicably be read or reconstructed. Burning or pulverizing such papers are also options where appropriate.
2. Destruction or erasure of electronic media containing consumer information so that the information cannot practicably be read or reconstructed.
3. After due diligence,[2] entering into and monitoring compliance with a contract with another party engaged in the business of record destruction to dispose of material in a manner consistent with this directive.

This policy does not require that the consumer reports information be disposed of. Rather, it specifies the action to be taken whenever such disposal occurs. Questions regarding the disposal of consumer reports information should be directed to the Administrator or the Administrator's designee.

Legal Reference:	FTC Rule on Disposal of Consumer Report Information and Records, 16 CFR Part 682
Date of Adoption: Updated:	May 19, 2020

[1] "The term 'consumer report' means any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for . . . employment purposes." Fair Credit Reporting Act, 15 U.S.C. § 1681a(3).

[2] The FTC rule states: "In this context, due diligence could include reviewing an independent audit of the disposal company's operations and/or its compliance with this rule, obtaining information about the disposal company from several references or other reliable sources, requiring that the disposal company be certified by a recognized trade association or similar third party, reviewing and evaluating the disposal company's information security policies or procedures, or taking other appropriate measures to determine the competency and integrity of the potential disposal company."

D. Prohibition on Aiding and Abetting Sexual Abuse

An employee, contractor, or agent of ESU #13 is prohibited from assisting another ESU #13 employee, contractor or agent in obtaining a new job if the individual knows or has probable cause to believe, that such other employee, contractor, or agent engaged in sexual misconduct in violation of the law.

"Assisting" does not include the routine transmission of administrative and personnel files.

Exceptions to giving such assistance may only be made where the exception is authorized by the Every Student Succeeds Act (for example, where the matter has been investigated by law enforcement and the person has been exonerated and approved by the Administrator or designee.)

Legal Reference:	ESSA sec. 8038, § 8546
Date of Adoption: Updated:	May 19, 2020

E. Workplace Privacy Policy

1. ESU #13 will abide by the Nebraska Workplace Privacy Act and will not:

   a. Require or request that an employee or applicant provide or disclose any user name or password or any other related account information in order to gain access to the employee's or applicant's personal Internet account by way of an electronic communication device;
   b. Require or request that an employee or applicant log into a personal Internet account by way of an electronic communication device in the presence of ESU #13 in a manner that enables ESU #13 to observe the contents of the employee's or applicant's personal Internet account or provides ESU #13 access to the employee's or applicant's personal Internet account;
   c. Require an employee or applicant to add anyone, including ESU #13, to the list of contacts associated with the employee's or applicant's personal Internet account or require or otherwise coerce an employee or applicant to change the settings on the employee's or applicant's personal Internet account which affects the ability of others to view the content of such account;
   d. Take adverse action against, fail to hire, or otherwise penalize an employee or applicant for failure to provide or disclose any of the information or to take any of the actions prohibited by the Workplace Privacy Act.
   e. Require an employee or applicant to waive or limit any protection granted under the Workplace Privacy Act as a condition of continued employment or of applying for or receiving an offer of employment.

Notwithstanding anything to the contrary, all employees must abide by the ESU #13 technology policies, procedures and guidelines, including the ESU #13 Internet Use policy and/or practice. Pursuant to the Workplace Privacy Act, ESU #13 may also:

a. Monitor, review, access, or block electronic data stored on an electronic communication device supplied by or paid for in whole or in part by ESU #13 or stored on the ESU #13 network, to the extent permissible under applicable laws;
b. Access information about an employee or applicant that is in the public domain or is otherwise obtained in compliance with the Workplace Privacy Act;
c. Conduct an investigation or require an employee to cooperate in an investigation if ESU #13 has specific information about potentially wrongful activity taking place on the employee's personal Internet account, for the purpose of ensuring compliance with applicable laws, regulatory requirements, or prohibitions against work-related employee misconduct;
d. Any other reason permitted by the Workplace Privacy Act.

Legal Reference:	Nebraska Statutes: §48-3501 to 48-3511
Date of Adoption: Updated:	May 19, 2020