NEBRASKA DEPARTMENT OF EDUCATION

ADMINISTRATIVE MEMORANDUM #707

ISSUED: FEBRUARY, 2014

TO: NDE Staff

FROM: Dr. Matthew L. Blomstedt, Commissioner of Education

SUBJECT: DATA SECURITY

FOR ASSISTANCE: Contact Data, Research and Evaluation Administrator at 471-4740

PURPOSE

NDE has a legal and ethical responsibility to protect the privacy and security of education data, including personally identifiable information. The purpose is to mitigate the risks from inadvertent disclosure of inappropriate, sensitive or protected data or computer security breaches by providing a plan of action for any incidences of this nature that occur.

Policy

- Administrative Memorandum #711 covers Student and Staff Data Privacy and Confidentiality requirements
- Administrative Memorandum #304 covers Employee Responsibility for Reporting Lost, Stolen or Missing State Property
- Administrative Memo #606 covers Public Access to Records & Reproduction Costs
- Administrative Memo #709 covers Data Collections
- Administrative Memo #710 covers Records Retention

References

- Family Educational Rights and Privacy Act (FERPA – Title 34 Code of Federal Regulations Part 99) [Note: FERPA does not address breach issues but requires recordation of each incidence of data disclosure.]
- Financial Data Protection and Consumer Notification of Data Security Breach Act of 2006 [Neb. Rev. State 87-802 through 807]
- Nebraska Information Technology Commission (NITC) Standards and Guidelines
    - 8-101 Information Security Policy
    - 8-102 Data Security Standard
    - 8-301 Password Standard
    - 8-401 Incident Response and Reporting Standard
- National Institute of Standards and Technology (NIST) Special Publication 800-61

Scope

- Applies to all NDE employees. Data Security must be addressed in the contracts for external vendors where appropriate and applicable.

Definitions

Data Breach A data breach is any instance in which there is an unauthorized release or access of personally identifiable information or other information not suitable for public release. A data breach can include: hackers accessing data; lost, stolen, or temporarily misplaced equipment; employee negligence; and policy and/or system failure.

Computer Security Incident A violation or imminent threat of computer security policies, acceptable use policies, or standard security practices

Incident Response: A documented process for detecting security breaches, minimizing loss and destruction, mitigating exploited weaknesses, and restoring computing services.

Personally Identifiable Information (PII)

Personally identifiable information, as defined in FERPA, includes, but is not limited to:

- a student's name;
- the name of the student's parent or other family members;
- the address of the student or student's family;
- a personal identifier, such as the student's Social Security number, student number, or biometric record;
- other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name;
- other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; and
- information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates.

Sensitive Information: Also known as secure data or nonpublic data, sensitive data includes personally identifiable information about students and clients, eligibility for free and/or reduced lunch programs, health information, Social Security numbers for adults and students, certification investigation documents in accordance with NDE Rule 29, birth certificates, and bank account information found on checks.

Staff Roles and Responsibilities

Every employee has an obligation and responsibility to protect sensitive information. These include:

- Keeping sensitive information in a locked or secure location when not in use.
- Arranging your workspace or organizing your work area to protect sensitive information.

- Not using or collecting Social Security numbers unless required to do so by law or regulation or as necessary and approved by the Commissioner or Deputy.
- Protecting passwords by never sharing or keeping in an easily accessible place or file.
- Accessing sensitive information only when authorized. See Administrative Memorandum #711 for approval process.
- Never putting sensitive information on private computers, laptops, tablets, phones, or memory drives. Sensitive information on official mobile devises is allowed if authorized by the appropriate Leadership Council member.
- Never sending Social Security numbers or personally identifiable information in emails unless encrypted or on a secure system.
- Never divulging, copying, releasing, selling, loaning, altering or destroying sensitive information without authorization.
- Destroying or rendering unusable any physical document (e.g. memos, reports, microfilm, microfiche) or any electronic storage medium (e.g., USB key, CD, DVD, tape, diskette) before it is discarded. (NOTE: Always consult Administrative Memo #710 and the appropriate records retention schedule before destroying or discarding documents and records).

Every employee has an obligation and responsibility to report any activities they suspect may have compromised sensitive information to their immediate supervisor or Leadership Council Member who in turn must report it to their network services staff and the Commissioner or Deputy.

NDE has adopted and is implementing the Nebraska Information Technology Commission (NITC} Standards and Guidelines for data security that include:

- 8-101 Information Security Policy
- 8-102 Data Security Standard
- 8-301 Password Standard
- 8-401 Incident Response and Reporting Standard

These guidelines cover all network services, computer hardware and software, mobile devices on which sensitive data is maintained in NDE.