DATA GOVERNANCE AND SECURITY

To accomplish the district's mission and comply with the law, the district must collect, create and store information. Accurately maintaining and protecting this data is important for efficient district operations, compliance with laws mandating confidentiality, and maintaining the trust of the district's stakeholders. All persons who have access to district data are required to follow state and federal law, district policies and procedures, and other rules created to protect the information.

Definitions

Confidential Data/Information B Information that the district is prohibited by law, policy or contract from disclosing or that the district may disclose only in limited circumstances. Confidential data includes, but is not limited to, personally identifiable information regarding students and employees.

Critical Data/Information B Information that is determined to be essential to district operations and that must be accurately and securely maintained to avoid disruption to district operations. Critical data is not necessarily confidential.

Responsibility and Data Stewardship

All district employees, volunteers and agents are responsible for accurately collecting, maintaining and securing district data including, but not limited to, information that is confidential or is critical to district operations.

Information Security Officer

Eric Campbell [Technology Director] is the district's information security officer (ISO) and reports directly to the superintendent or designee. The district's information security officer is directed to create and review district procedures on collecting and protecting district data including, but not limited to, securely maintaining confidential and critical information. The ISO is responsible for implementing and enforcing the district's security policies and procedures applicable to electronic data and suggesting changes to these policies and procedures to better protect the confidentiality and security of district data. The ISO will work with the district's technology department to advocate for resources and implement best practices to secure the district's data.

Principal [title] is the district's alternate ISO and will assume the responsibilities of the ISO when the ISO is not available.

Data Managers

All district administrators are data managers for all data collected, maintained, used and disseminated under their supervision as well as data they have been assigned to manage in the district's data inventory. Data managers will monitor employee access to the information to ensure that confidential information is accessed only by employees who need the information to provide services to the district and that confidential and critical information is modified only by authorized employees. Data managers will assist the ISO in enforcing district policies and procedures regarding data management.

Confidential and Critical Information

The district will collect, create or store confidential information only when the superintendent or designee determines it is necessary. The district will provide access to confidential information to appropriately trained district employees and volunteers only when the district determines that such access is necessary for the performance of their duties. The district will disclose confidential information only to authorized district contractors or agents who need access to the information to provide services to the district and who agree not to disclose the information to any other party except as allowed by law and authorized by the district.

District employees, contractors and agents will notify the ISO or designee immediately if there is reason to believe confidential information has been disclosed to an unauthorized person or any information has been compromised, whether intentionally or otherwise. The ISO or designee will investigate immediately and take any action necessary to secure the information, issue all required legal notices and prevent future incidents. When necessary, the district's superintendent, ISO or designee is authorized to secure resources to assist the district in promptly and appropriately addressing a security breach.

Likewise, the district will take steps to ensure that critical information is secure and is not inappropriately altered, deleted, destroyed or rendered inaccessible. Access to critical information will only be provided to authorized individuals in a manner that keeps the information secure.

All district staff, volunteers, contractors and agents who are granted access to critical and confidential information are required to keep the information secure and are prohibited from disclosing or assisting in the unauthorized disclosure of confidential information. All individuals using confidential and critical information will strictly observe protections put into place by the district including, but not limited to, limiting access to electronic files, updating and maintaining the confidentiality of password protections, encrypting and redacting information, and disposing of information in a confidential and secure manner.

Using Online Services and Applications

District staff members are encouraged to research and utilize online services or applications to engage students and further the district's education mission. However, before any online service or application is purchased or used to collect or store confidential or critical information, including confidential information regarding students or employees, the ISO or designee must approve the use of the service or application and verify that it meets the requirements of the law and Board policy and appropriately protects confidential and critical information. This prior approval is also required when the services are obtained without charge.

Training

In accordance with law, all school employees will receive annual training in the confidentiality of student records.

Data Retention and Deletion

The ISO or designee shall establish a retention schedule for the regular archiving and deletion of data stored on district technology resources. The retention schedule must comply with the *Public School District Records Retention Manual* as well as the *General Records Retention Manual* published by the Missouri Secretary of State.

Litigation Hold

In the case of pending or threatened litigation, the district's attorney will issue a litigation hold directive to the superintendent or designee. The litigation hold directive will override any records retention schedule that may have otherwise called for the transfer, disposal or destruction of relevant documents until the hold has been lifted by the district's attorney. E-mail and other technology accounts of separated employees that have been placed on a litigation hold will be maintained by the district's information technology department until the hold is released. No employee who has been notified of a litigation hold may alter or delete any electronic record that falls within the scope of the hold. Violation of the hold may subject the individual to disciplinary actions, up to and including termination of employment, as well as personal liability for civil and/or criminal sanctions by the courts or law enforcement agencies.

Consequences

Employees who fail to follow the law or district policies or procedures regarding data governance and security may be disciplined or terminated. Volunteers may be excluded from providing services to the district. The district will end business relationships with any contractor who fails to follow the law, district policies or procedures, or the confidentiality provisions of any contract. In addition, the

district reserves the right to seek all other legal remedies, including criminal and civil action and seeking discipline of an employee's teaching certificate.

The district may suspend all access to data or use of district technology resources pending an investigation. Violations may result in temporary, long-term or permanent suspension of user privileges. The district will cooperate with law enforcement in investigating any unlawful actions. The superintendent or designee has the authority to sign any criminal complaint on behalf of the district.

Any attempted violation of district policies, procedures or other rules will result in the same consequences, regardless of the success of the attempt.

* * * * * * *

Note: ***The reader is encouraged to check the index located at the beginning of this section for other pertinent policies and to review administrative procedures and/or forms for related information.***

Adopted: 11-16-17

Revised:

Cross Refs: BDC, Closed Meetings, Records and Votes
BDDL, Release of Information
DJF, Purchasing
GBEBC, Criminal Background Checks
GBL, Personnel Records
GBLB, References
IGBA, Programs for Students with Disabilities
JHDA, Surveying, Analyzing or Evaluating Students
JO, Student Records
KI, Public Solicitations/Advertising in District Facilities

Legal Refs: " 43.540, 109.260, 160.261, 210.150, .865, 407.1500, 576.050, 610.010 - .028, RSMo.
The Children's Online Privacy Protection Act, 15 U.S.C. 6501 - 6506
Federal Privacy Act of 1974, 5 U.S.C. ' 552a
E Sign Act of 2000, 15 U.S.C. ' 7001
Fair Credit Reporting Act, 15 U.S.C. ' 1681a
Family Educational Rights and Privacy Act, 20 U.S.C. ' 1232g

Individuals with Disabilities Education Act, 20 U.S.C. " 1400 - 1417
Protection of Pupil Rights Amendment, 20 U.S.C. ' 1232h
The Elementary and Secondary Education Act of 1965, 20 U.S.C. ' 7926
29 C.F.R. ' 1630.14

Dent-Phelps R-III School District, Salem, Missouri