DATA GOVERNANCE AND SECURITY
(Data Management)

The effective education of students and management of district personnel often require the district to collect information, some of which is considered confidential by law and district policy. In addition, the district maintains information that is critical to district operations and that must be accurately and securely maintained to avoid disruption to district operations. Because it is important that the district, district employees and all users of district data are good stewards of this information, the district has created a program to ensure that all data, including confidential and critical information, is accessed and maintained appropriately.

Definitions

Confidential Data/Information: 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 (PII) regarding students and employees.

Critical Data/Information: 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.

Data Inventory and Classification

The information security officer (ISO) or designee will identify all systems containing district data, such as student information systems, financial systems, payroll systems, transportation systems, food-service systems, e-mail systems, instructional software applications and others. The ISO or designee will identify the data files and data elements maintained in those files within the systems and identify confidential and critical information the district possesses or collects. All district employees are directed to assist the ISO or designee in identifying confidential and critical information and explain the sources of the data and the purposes for which the data is collected and used so that file classification is accurate.

Once the data files and data elements are identified, the ISO will classify the data as confidential or critical so that those files and the information they contain can be more closely monitored. Additional classifications may be added as necessary to assist in monitoring and data governance.

Once the data is classified, the ISO or designee will create a data inventory. The data inventory will include documentation of the location of the files, the persons assigned to manage the files, and the employees or employee categories that have access to the files. The ISO will maintain the district's data inventory in both electronic and printed form and will update it annually.

Creating, Accessing and Using Data

Data will be collected, maintained and used by the district only when it is needed for the district to fulfill its education mission. Authorized district employees, volunteers, district agents and vendors may create, access and use district data when necessary to provide services to the district, but they must do so in a manner that ensures that the data is accurate, complete, timely and relevant. Authorized users must obtain permission from the district to use the data for other purposes, including personal purposes.

The security of confidential information, including confidential PII and critical information, is particularly important, and authorized users of this information may access the information only when necessary to perform their duties for the district. The district's security administrator will work with the superintendent and relevant supervisors to determine which persons are authorized to create, access and use confidential or critical information. Confidential and critical information can only be used in accordance with state and federal confidentiality laws and district policies and procedures regarding confidential information. Confidentiality laws include, but are not limited to, the Family Educational Rights and Privacy Act, the Protection of Pupil Rights Amendment, the Children's Online Privacy Protection Act, the Missouri Safe Schools Act, the Missouri Sunshine Law, and various criminal statutes. Relevant policies include, but are not limited to, the policies cross-referenced in policy EHBC.

Unless permission has been granted by the security administrator, no employee, vendor or other person may remove confidential or critical data from the district's premises or the district's network, remove a device containing confidential or critical data from the district's premises, or modify or copy confidential or critical data for use outside the district. If permission is given, the data may be accessed only on a district-provided device with appropriate security controls or through a secure virtual private network (VPN). When users access confidential or critical data from a remote location, the user must take precautions to ensure that the confidential or critical data is not downloaded, copied or otherwise used in a manner that would compromise the security and confidentiality of the information.

Maintaining Data

Confidential and critical information will be saved and maintained in a secure manner using encryption or other password-protected security measures. Likewise, when data is transmitted, the district will use encryption or password-protected security measures.

Dissemination and Disclosure of Data

District data is collected and maintained to further the district's education mission. A district employee or other authorized user of the district's data may use and disseminate it in furtherance of his or her job duties with the district as long as confidentiality laws and district policies and procedures are followed. Authorized users must obtain permission from the district before disseminating data for other purposes, including personal purposes. All requests for district information by the media or members of the public under the Missouri Sunshine Law will be directed to the district's custodian of records, who will respond to those requests as required by law.

Authorized users of confidential information are prohibited from disseminating the information to unauthorized persons unless the user is required by law to share the information, is authorized in Board policy or procedure to do so, or is directed by his or her supervisor to do so. Confidential and critical information that is disseminated electronically must be encrypted or password-protected.

In some circumstances confidential information can be shared when it has been redacted or altered so that the information is not personally identifiable and is no longer considered harmful or an invasion of privacy. An authorized user has the responsibility of verifying with his or her supervisor or the district security administrator whether the information has been sufficiently altered or redacted prior to releasing the information.

Authorized users of critical information that is not confidential may disseminate the information in accordance with their duties or when required by law, but such dissemination must be done in a manner that protects the security and integrity of the information.

Retaining, Archiving and Destroying Data

Retaining and Archiving Information

The ISO, in consultation with the district's custodian of records, data managers and other qualified staff, 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 Records Retention Schedule* and the *General Records Retention Schedule* published by the Missouri Secretary of State.

Permanent records may be maintained by storing such records in a digital or electronic format for the manufacturer-suggested or recommended period of time. If the ISO chooses to store permanent records electronically, the district will follow all guidelines, suggestions or recommendations set forth by the manufacturer.

Litigation Hold

If the district's attorney notifies the district that, due to litigation, certain records cannot be deleted, the directive will be communicated to the ISO and the relevant staff. Once notified, no employee, volunteer, agent or vendor is allowed to alter, delete or destroy any information that might be relevant to the pending litigation, regardless of how the information is maintained.

Destruction of Information

Once data is no longer needed, the ISO will work with the data managers to ensure that it is appropriately destroyed. Special care will be taken to ensure that confidential information is destroyed appropriately and in accordance with law. Confidential paper records will be destroyed using methods that render them unreadable, such as shredding. Confidential digital records will be destroyed using methods that render the record un-retrievable. The ISO is authorized to use the district's procurement process to contract with an independent contractor with expertise in the area for records disposal.

Removal of Information from Devices

Before a computer, tablet or other device is sold as surplus property, transferred to another person or used for a different purpose than originally intended, the ISO or designee will remove all confidential and critical information from the device.

Monitoring Release of Confidential Information

The ISO will work with data managers to monitor how confidential data is used and released and to verify that district policies and procedures governing access to the information are being followed.

Monitoring Service Providers

The district uses attorneys and other specialized service providers as independent contractors. When necessary, these service providers are given access to confidential and critical information electronically or in other forms. The ISO will periodically audit the agreements and working relationships with these contractors to determine whether access to confidential or critical information is necessary and ensure that the data is appropriately used and protected.

Monitoring Vendors of Electronic Services

District employees are prohibited from installing software or using any online system that stores, collects or shares confidential or critical data until the ISO approves the vendor and the software or service used. This applies even if the software or system is free. All users must comply with

copyright and licensing requirements and are prohibited from copying or using district licenses at home or for personal use unless authorized by the ISO.

The ISO will establish a process for ensuring that software and systems the district purchases or uses comply with the district's data security principles. The ISO will maintain a copy of all contracts with vendors that impact the district's data or data security. All contracts with vendors will conform with the requirements of state and federal law and will require the vendor to appropriately secure district data.

Before authorizing the use of a vendor, software or service in which confidential or critical data will be stored, collected or shared, the ISO will ensure that the vendor, software or service will adequately protect the district's data and act in the district's interests. All vendors, software or services used must conform to the following unless otherwise authorized by the superintendent or Board:

1. The district continues to own the data shared with the vendor, and all data must be available to the district upon request.

2. The vendor's access to and use of district data is limited; the data cannot be used for marketing, advertising or data mining; and the data cannot be shared with third parties unless allowed by law and authorized by the district.

3. If metadata is collected, it will be protected to the same extent as the district's confidential or critical information.

4. District data will be stored only on servers in the United States.

5. District data will be maintained in a secure manner by applying appropriate technical, physical and administrative safeguards to protect the data.

6. The vendor, software or service will detail how and when district data will be destroyed.

7. In the event of a data breach, the vendor will immediately notify the ISO. Further, the vendor will assume liability for any breach of data when such data is being collected or manipulated by the vendor or is in the possession or control of the vendor.

8. There must be consequences and penalties if the vendor or online system discloses or uses district data inappropriately, without authorization or in violation of the law.

9. The district is entitled to monitor and audit the vendor or online system to ensure compliance with the agreement.

10. Products and services provided by the vendor will be provided in a manner that accommodates persons with disabilities in accordance with the requirements of the Americans with Disabilities Act and other applicable state and federal laws.

The ISO or designee will periodically review the overall performance of vendors and determine whether the:

1. Vendor is in compliance with the contract.
2. District is receiving value.
3. District's data is maintained securely.
4. Vendor has addressed any concerns raised by the district.

Free Electronic Services

District employees are prohibited from sharing confidential information or requiring students or other employees to share their confidential information using free online services unless the ISO has verified that the service complies with the same expectations as those listed in this procedure for paid vendor services and that the service is operated in compliance with confidentiality laws and district policies.

Security Awareness Program

The ISO will work with data managers to develop and implement a security and privacy awareness program for all staff who have access to the district's confidential and critical data as part of their employment. The goals of the security awareness program are to:

1. Enhance district data security by improving awareness of the need to protect system resources.

2. Develop skills and knowledge so computer users can perform their jobs more securely.

3. Build in-depth knowledge, as needed, to design, implement or operate security programs.

The program will include training on a recurring basis, communication of privacy policies, and communication of the process for reporting privacy incidents and submitting complaints.

Electronic Access Banners

The security and privacy awareness program will include the use of electronic messages (electronic access banners) that appear when users access district data electronically and that regularly remind users of privacy and security information, including the following notices:

1. The user is accessing a district-provided information system.

2. Usage of the system may be monitored, recorded and subject to auditing.

3. Unauthorized use of the system is prohibited and may be subject to criminal and civil penalties.

4. Use of the system constitutes agreement with the terms listed on the banner.

* * * * * * *

Note: The reader is encouraged to review policies and/or forms for related information in this administrative area.

Implemented: November 29, 2017

Revised:

Boonville R-I School District, Boonville, Missouri