Sedalia #200 School District

Technology/Data Governance Manual

Contents

Introduction

The District is committed to protecting our students' and staffs' privacy through maintaining strong privacy and security protections. The privacy and security of this information is a significant responsibility and we value the trust of our students, parents, and staff.

The SSD Data Governance Manual includes information regarding the data governance team, data and Information governance, applicable Board of Education policies, procedures and forms, as well as applicable appendices and referenced supplemental resources.

This manual outlines how operational and instructional activity shall be carried out to ensure the District's data is accurate, accessible, consistent, and protected. The document establishes who is responsible for information under various circumstances and specifies what procedures shall be used to manage and protect it.

Definitions of terminology can be found in Appendix A: Definitions.

The Sedalia School District Data Governance Manual shall be a living document. To make the document flexible details are outlined in the appendices and referenced supplemental resources. All modifications will be posted on the District's website under the district tab.

Data Governance Team

The SSD Data Governance team consists of the superintendent and/or designees.
Members of the Data Governance Team will act as data stewards for all data under their direction. The Superintendent or designee will act as the Information Security Officer (ISO), with assistance from the Director of Technology. All members of the district administrative team will serve in an advisory capacity as needed.

Purpose

Sedalia 200 Schools' technology exists for the purpose of enhancing the educational opportunities and achievement of district students.

Technology assists with the professional enrichment of the staff and increases engagement of students' families and other patrons of the district, all of which may positively impact student achievement.

To accomplish the district's mission and to comply with the law, the district may need to collect, create and store confidential information, including information regarding students, parents/guardians, employees, applicants for employment and others. The district will only do so when necessary and will take measures to keep this information confidential as required by law.

It is the policy of Sedalia 200 Schools that data or information in all its forms--written, electronic, or printed--is protected from accidental or intentional unauthorized modification, destruction or disclosure throughout its life cycle. This protection includes an appropriate level of security over the equipment, software, and practices used to process, store, and transmit data or information.

Per Board of Education Policy 2400 the superintendent or designee is directed to create and review district procedures on securely maintaining confidential information and to provide adequate training to employees and others with access to the information. In addition, all employees and authorized district contractors or agents using personal information will strictly observe protections put into place by the district.

Scope

The data security policy, standards, processes, and procedures apply to all students and employees of the district, contractual third parties and agents of the district, and volunteers who have access to district data systems or data. This policy applies to all forms of Sedalia 200 Schools' data and information, including but not limited to:

- Speech, spoken face to face, or communicated by phone or any current and future technologies
- Hard copy data printed or written
- Communications sent by post/courier, fax, electronic mail, text, chat and or any form of social media
- Data stored and/or processed by any electronic device, including servers, computers, tablets, mobile devices
- Data stored on any type of internal, external, or removable media or cloud based services
- The terms data and information are used separately, together, and interchangeably
- throughout the policy, the intent is the same
- Any computer, laptop, mobile device, printing and/or scanning device, network
- appliance/equipment, AV equipment, server, internal or external storage, communication device or any other current or future electronic or technological device may be referred to as systems, assets or resources
- All involved systems and information are assets of Sedalia Schools shall be
- protected from misuse, unauthorized manipulation, and destruction

Regulatory Compliance

The district will abide by any law, statutory, regulatory, or contractual obligations affecting its data systems (see Appendix B: Laws, Statutory, and Regulatory Security Requirements). Sedalia Schools complies with all applicable regulatory acts including but not limited to the following:

- Children's Internet Protection Act (CIPA)
- Children's Online Privacy Protection Act (COPPA)
- Family Educational Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Protection of Pupil Rights Amendment (PPRA)
- Missouri State Statutes: §407.1500 (Breach of Security); §109.200, §109.210, §109.310 (Records)

Data User Compliance

The Data Governance Manual applies to all users of Sedalia 200 Schools' information including: employees, staff, students, volunteers, and authorized district contractors or agents. All data users are to maintain compliance with Board of Education Policies 2400 (Privacy Protection), 6320 (Technology Usage) and all policies, procedures, and resources as outlined within this Data Governance Manual and Board of Education Policy.

A consistently high level of personal responsibility is expected of all users granted access to the district's technology resources. Any violation of district policies or procedures regarding technology usage may result in temporary, long-term or permanent suspension of user privileges.

User privileges may be suspended pending investigation into the use of the district's technology resources.

Employees may be disciplined or terminated, and students suspended or expelled, for violating the district's technology policies and procedures. Any attempted violation of the district's technology policies or procedures, regardless of the success or failure of the attempt, may result in the same discipline or suspension of privileges as that of an actual violation. The district will cooperate with law enforcement in investigating any unlawful use of the district's technology resources.

Furthermore, the district may seek all legal recourse against any person who accesses confidential information without authorization or who fails to maintain the confidentiality of confidential information.

District employees who violate district policies or procedures regarding the confidentiality of information may be disciplined and/or terminated.

Possible disciplinary/corrective action may be instituted for, but is not limited to, the following:

- Unauthorized disclosure of PII or Confidential Information
- Sharing your user IDs or passwords with others or using another person's ID or password (exception for authorized technology staff for the purpose of support)
- Unauthorized use of credentials to access student or employee privacy
- The unauthorized copying of system files
- Attempting to secure a higher level of privilege without authorization
- The intentional unauthorized altering, destruction, or disposal of district information, data and/or systems. This includes the unauthorized removal of technological systems such as but not limited to: mobile devices, internal or external storage, computers, servers, backups or other media, that may contain PII or confidential information
- The introduction of computer viruses, hacking tools or other disruptive or destructive programs

Data Lifecycle

Data Governance is necessary at each phase in the data lifecycle. This lifecycle starts at evaluating the need for data collection and ends when the data is destroyed. It is important that appropriate safeguards, policies, procedures and practices are in place for each phase of the data lifecycle.

Identifying Need & Assessing Systems for District Requirements

To accomplish the district's mission and to comply with the law, the district may need to collect, create and store confidential information, including information regarding students, parents/guardians, employees, applicants for employment and others. The district will only do so when necessary and will take measures to keep this information confidential as required by law.

Management and Storage

Systems Security

District employees will only access personally identifiable confidential information if necessary to perform their duties. The district will only disclose this information 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 (BOE Policy 2400). Therefore, systems access will only be given on an as needed basis as determined by the data manager and ISO. Further information regarding Electronic Access Security Controls is contained in the Security/Protection section of this manual.

Security/Protection

Risk Management

A risk analysis of all Sedalia School District data networks, systems, policies, and procedures shall be an ongoing process or as requested by the Superintendent, ISO or Director of Technology. The product of the risk analysis will be referred to as the risk assessment. The risk assessment shall be an ongoing process to mitigate identified threats and risk.

Logon Banners

The district will ensure that staff, students and parents using district systems are aware of the district data security policies. When possible, district systems users will acknowledge the full technology usage agreement prior to accessing all district technical systems.

Physical Security Controls

Access to areas in which information processing is carried out shall be restricted to only authorized individuals (see appendix F: Physical Security Controls).
No technological systems shall be disposed of or moved without adhering to the appropriate procedures (see Appendix G: Asset Management).

Inventory Management

The district shall maintain a process for inventory control in accordance to federal and state requirements and Board policy. All district assets will be maintained in inventory and verified through the regular inventory verification process (see Appendix G: Asset Management).

Virus, Malware, Spyware, Phishing and SPAM Protection

The District uses a multi-layered approach to ensure that all electronic files are appropriately scanned for viruses, malware, spyware, phishing and SPAM. These include, but are not limited to, enterprise virus/malware/ spyware software, group policy, gateways, firewalls, and content filter.

Users shall not turn off or disable district protection systems or to install other systems (see Appendix I: Virus, Malware, Spyware, Phishing and SPAM Protection).

Electronic Access Security Controls

District employees will only access personally identifiable and/or confidential information if necessary to perform their duties.

The district will only disclose this information 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 (BOE Policy 2400).
All staff acknowledge district policies, including Technology Usage and Data Privacy during orientation as well as annually.

Mechanisms to control access to PII, confidential information, internal information and computing resources include, but are not limited to, the following methods:

- Identification/Authentication: Unique user identification (user ID) and authentication are required for all systems that maintain or access PII, confidential information, and/or internal information.
- Users will be held accountable for all actions performed on the system with their User ID. User accounts and passwords shall not be shared.
- Authorization: Access controls are maintained through a partnership between the technology department, human resources (HR) and data managers.

Employee Users

All new employee accounts are authorized through an HR hiring process (see Appendix J: Account Management). Role-based permissions are used to establish access to all systems (see Appendix J: Data Access Roles and Permissions).
If an employee requires additional access, permission must be given and approved by the appropriate data manager.

Contractors/Vendors

All contractor/vendor access must be approved in accordance to district policy.
All contractors/vendors accessing district data will be considered on premise users. Once the approval has been obtained, the technology department will create the account, only granting access to the server/application that the contractor/vendor supports.

Password Security

The District will enforce secure passwords for all systems within their control.
At a minimum, staff passwords shall be changed each semester (see Appendix K: Password Security). When possible, the district will utilize Active Directory Integration to maintain optimal account security controls. District computers will auto lock after being idle for 10 minutes and require the user to re-enter their password.

Remote Access

Access into the District's network from outside is strictly prohibited without explicit authorization from the ISO.   PII, confidential information and/or Internal Information that is stored or accessed remotely shall maintain the same level of protections as information stored and accessed within District's network. In the event that remote access is needed by a contractor/vendor, access must be approved by the ISO. The Director of Technology or the Network Administrator will establish the contractor account, only granting access to the server/application that the contractor/vendor supports.

Securing Data at Rest and Transit

District data security applies to all forms of data, including data stored on devices, data in transit and data stored on additional resources. Regular transmission of student data to services such as a learning management system is managed by the technology department using a secure data transfer protocol. Users must ensure that they are securely storing their data. Guidelines have been established for Cloud Storage and File Sharing, External Storage Devices, File Transmission Practices. These guidelines can be found in the Usage and Dissemination section below (see Appendix E: Securing Data at Rest and Transit).

Usage and Dissemination

A consistently high level of personal responsibility is expected of all users granted access to the district's technology resources. All employees and authorized district contractors or agents using personal information will strictly observe protections put into place by the district including, but not limited to, maintaining information in locked rooms or drawers, limiting access to electronic files, updating and maintaining the confidentiality of password protections, encrypting and censoring information, and disposing of information in a confidential and secure manner (BOE Policy 2400).

All users are responsible for the security and integrity of the data they create, store or access. Users are expected to act as good stewards of data and treat data security and integrity with a high degree of responsibility and priority. Users must follow all guidelines outlined with Board policies, specifically Technology Usage (6320, 6530, and 6531), Data Privacy (6320), Staff Conduct (4630, 6320), and Student Record (2831). District employees, contractors and agents will notify the superintendent or designee immediately if there is reason to believe confidential information has been disclosed to an unauthorized person or to an authorized person in an unauthorized manner, whether intentionally or otherwise.

Securing Data at Rest and Transit

All staff and students that log into a district issued computer will be provided with several options for data storage and transmission.

Staff and students will need to ensure that they are securely storing their data.

Staff and students will be able to store data on their local device. It is important to note that this data is not a part of the district's continuity plan, and thus will not be backed up by the district's backup solution.Staff and students may also have a mapped folder. These folders allow storage of documents to district file servers and cloud-based resources. Access to these files is restricted to the staff and students assigned membership to the folder and district enterprise administrator accounts.

Cloud Storage and File Sharing

The term "Cloud Storage" is used to define all types of remote server storages accessed by users through the internet. All staff and students are provided with a Google Apps for Education account that provides unlimited storage.

Users are responsible for all digital content on their district provided Google Apps for Education Drive (see Appendix E: Securing Data at Rest and Transit).

File Transmission Practices

Staff are responsible for securing sensitive data for transmission through email or other channels with encryption or a password.

Staff should never transmit files labeled classified, confidential, or restricted through email or third party file transfer services without district approval.

When possible, staff should de-identify or censor any PII or confidential information prior to transmission.

Regular transmission of student data to services such as a learning management system is managed by the technology department using a secure data transfer protocol (see Appendix E: Securing Data at Rest and Transit).

Mass Data Transfers

Downloading, uploading or transferring PII, confidential information, and internal information between systems shall be strictly controlled.

Requests for mass download of, or individual requests for, information for research or any other purposes that include PII shall be in accordance with Board policy 6530, and 6531.

All other mass downloads of information shall be approved by the ISO and include only the minimum amount of information necessary to fulfill the request.

Printing

When possible, staff should de-identify or censor any PII or confidential information prior to printing. PII and confidential information shall not be downloaded, copied or printed indiscriminately or left unattended and open to compromise.

Oral Communications

Staff shall be aware of their surroundings when discussing PII and confidential information. This includes, but is not limited to, the use of cellular telephones in public areas. Staff shall not discuss PII or Confidential Information in public areas if the information can be overheard.

Caution shall be used when conducting conversations in: semi-private rooms, waiting rooms, corridors, elevators, stairwells, cafeterias, restaurants, or public areas.

Training

The district shall maintain a data security training program that will include training for all staff on technology policies and procedures, including confidentiality and data privacy.

Archival and Destruction

District Data Destruction Processes

The district will regularly review all existing data stored on district provided storage for the purposes of ensuring data identification and appropriate destruction.
Data destruction processes will align with Policy 6531.
Data Retention: District data managers will regularly review systems and data to ensure that data that is no longer needed is destroyed. The following exceptions will be made:

- Data in an active litigation hold will be maintained until the conclusion of the hold.
- Employee home folder data will be maintained for 1 year after the final work day, unless HR approves for a district administrator to maintain access. Staff will be denied access the day after their last contract day. Staff and student Google drives will be retained for one year after they leave the district. Access will be denied by June 30th of the current school year.

Asset Disposal

The district will maintain a process for physical asset disposal in accordance to Board policy. The district will dispose of all assets containing PII, confidential, or internal information are disposed in a manner that ensures that this information is destroyed (see Appendix G: Asset Management).

Critical Incident Response

Controls shall ensure that the District can recover from any damage to or breach of critical systems, data, or information within a reasonable period of time.
Each school, department, or individual is required to report any instances immediately to the Superintendent, Director of Technology and/or Information Security Officer for response to a system emergency or other occurrence (for example, fire, vandalism, system failure, data breach and natural disaster) that damages/breaches data or systems.

Document Retention

The District's administrative procedure policies 6530 & 6531 Document Retention delineates the process for data retention for all district data including backup requirements. The District will maintain systems that provide near-line backup. These systems shall allow for the full recovery of critical systems in the event of a disaster. The district will test near-line backups quarterly.

Disaster Response

The District's Technology Disaster Recovery Plan outlines critical staff, responsibilities, and processes in the event of a disaster or critical data loss. District servers are backed up daily. (see Appendix L: Disaster Response Plan).

Data Breach Response

The Data Breach Response Plan enables the District to respond effectively and efficiently to a data breach involving personally identifiable information (PII), confidential or protected information, district identifiable information and other significant cybersecurity incident.
The Data Breach Response Plan shall include processes to validate and contain the security breach, analyze the breach to determine scope and composition, minimize impact to the users, and provide notification (see Appendix M: Data Breach Response Plan).

Appendix A
Definitions

Confidentiality: Data or information is not made available or disclosed to unauthorized persons or processes.
Data: Facts or information. Data can be in any form; oral, written, or electronic.
Data Integrity: Data is current, accurate and has not been altered or destroyed in an unauthorized manner.
Data Management: The development and execution of policies, practices, and procedures in order to manage the accuracy and security of district instructional and operational data in an effective manner.
Data Owner: User responsible for the creation of data. The owner may be the primary user of that information or the person responsible for the accurate collection/recording of data. Ownership does not signify proprietary interest, and ownership may be shared. The owner of information has the responsibility for:

- knowing the information for which she/he is responsible
- determining a data retention period for the information in according to Board policy and state statute
- ensuring appropriate procedures are in effect to protect the integrity, confidentiality, and availability of the data used or created
- reporting promptly to the ISO the loss or misuse of data
- initiating and/or implementing corrective actions when problems are identified.
- following existing approval processes for the selection, budgeting, purchase, and implementation of any digital resource

Information Security Officer: The Information Security Officer (ISO) is responsible for working with the superintendent, Data Governance Team, data managers, data owners, and users to develop and implement prudent security policies, procedures, and controls. The Information Security Officer will oversee all security audits and will act as an advisor to:

- data owners for the purpose of identification and classification of technology and data related resources.

Systems: Any computer, laptop, mobile device, printing and/or scanning device, network appliance/equipment, AV equipment, server, internal or external storage, communication device or any other current or future electronic or technological device, whether hosted by the district or provider.
Personally Identifiable Information (PII): Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.
Risk: The probability of a loss of confidentiality, integrity, or availability of information resources.User: The user is any person who has been authorized to read, enter, print or update information. A user of data is expected to:

- access information only in support of their authorized job responsibilities.
- comply with all data security procedures and guidelines.
- keep personal authentication confidential (user IDs, passwords, secure cards, PINs, access codes).

- report promptly to the Information Security Officer the loss or misuse of data.
- follow corrective actions when problems are identified.

Appendix B
Laws, Statutory, and Regulatory Security Requirements

CIPA: The Children's Internet Protection Act was enacted by Congress in 2000 to address concerns about children's access to obscene or harmful content over the Internet. CIPA imposes certain requirements on schools or libraries that receive discounts for Internet access or internal connections through the E-rate program.
Schools subject to CIPA have two additional certification requirements: 1) their Internet safety policies shall include monitoring the online activities of minors; and 2) as required by the Protecting Children in the 21st Century Act, they shall provide for educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyber bullying awareness and response. http://www.fcc.gov/guides/childrens-internet-protection-act

COPPA: The Children's Online Privacy Protection Act regulates operators of commercial websites or online services directed to children under 13 that collect or store information about children. Parental permission is required to gather certain information. www.coppa.org

FERPA: The Family Educational Rights and Privacy Act applies to all institutions that are recipients of federal aid administered by the Secretary of Education. This regulation protects student information and accords student's specific rights with respect to their data. http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

HIPAA: The Health Insurance Portability and Accountability Act applies to organizations that transmit or store Protected Health Information (PII). It is a broad standard that was originally intended to combat waste, fraud, and abuse in health care delivery and health insurance, but is now used to measure and improve the security of health information as well. http://www.hhs.gov/ocr/privacy/hipaa/understanding

PCI DSS: The Payment Card Industry Data Security Standard was created by a consortium of payment brands including American Express, Discover, MasterCard, and Visa. It covers the management of payment card data and is relevant for any organization that accepts credit card payments. www.pcisecuritystandards.org

PPRA: The Protection of Pupil Rights Amendment affords parents and minor students' rights regarding our conduct of surveys, collection and use of information for marketing purposes, and certain physical exams. http://www2.ed.gov/policy/gen/guid/fpco/ppra/index.html. These include the right to the following:

- Consent before students are required to submit to a survey funded in whole or in part by a program of the U.S. Department of Education that concerns one or more of the following protected areas:
    - Political affiliations or beliefs of the student or student's parent
    - Mental or psychological problems of the student or student's family
    - Sex behavior or attitudes
    - Illegal, anti-social, self-incriminating, or demeaning behavior

  - Critical appraisals of others with whom respondents have close family relationships
  - Legally recognized privileged relationships, such as with lawyers, doctors, or ministers
  - Religious practices, affiliations, or beliefs of the student or parents
  - Income, other than as required by law to determine program eligibility
- Inspect protected information surveys, instruments used to collect personal information for marketing or sales purpose, and instructional materials used as part of the educational curriculum. Missouri State Statutes:
- §407.1500 applies to a breach in security that results in the release of PII or otherwise protected information. This statute details expectations for investigation and notification.
- §109.210, §109.200, and §109.310 defines a record and addresses record retention and destruction.

Appendix C

Digital Resource Licensing/Use

All computer software developed by district employees or contract personnel on behalf of the District, licensed or purchased for district use is the property of the District and shall not be copied for use at home or any other location, unless otherwise specified by the license agreement.

- All staff must adhere to the following guidelines regarding digital resource licensing/use:
- Only approved district resources are to be used.
- District software licenses will be:
  - kept on file in the technology office.
  - accurate, up to date, and adequate.
  - in compliance with all copyright laws and regulations.
  - in compliance with district, state and federal guidelines for data security.
- Software installed on Sedalia School District systems and other electronic devices will have a current license on file or will be removed from the system or device.
- Resources with or without physical media (e.g. downloaded from the Internet, apps, or online) shall still be properly evaluated and licensed, if necessary, and is applicable to this procedure.
- Under no circumstances can staff act as a parental agent when creating student accounts for online resources; resources requiring this permission must be approved at district level.

Appendix D

Data Classification Levels

Personally Identifiable Information (PII)

PII is information about an individual maintained by an agency, including:

- Any information that can be used to distinguish or trace an individual‘s identity, such as name, social security number, date and place of birth, mother‘s maiden name, or biometric records.
- Any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Unauthorized or improper disclosure, modification, or destruction of this information could violate state and federal laws, result in civil and criminal penalties, and cause serious legal implications.

Confidential Information

Confidential Information is very important and highly sensitive material that is not classified as PII. This information is private or otherwise sensitive in nature and shall be restricted to those with a legitimate business need for access. Examples of confidential information may include: student records, personnel information, key financial information, proprietary information, system access passwords and encryption keys. Unauthorized disclosure of this information to individuals without a business need for access may violate laws and regulations, or may cause significant consequences for district, its staff, parents, students or other stakeholders.

Internal Information

Internal Information is intended for unrestricted use within the district and in some cases within affiliated stakeholders. This type of information is already widely-distributed within the district, or it could be distributed within the organization without advance permission from the information owner. Examples of Internal Information include internal policies and procedures and handbooks. Unauthorized disclosure of this information to outsiders may not be appropriate due to copyright, legal or contractual provisions.

Directory Information

Directory Information is information contained in an education record of a student that generally would not be considered harmful or an invasion of privacy if disclosed without the consent of a parent or eligible student. The school district designates the following items as directory information:

- General Directory Information
    - Student's name; date and place of birth; parents' names; grade level; enrollment status (e.g.,full-time or part-time); student identification number; user identification or other unique personal identifier used by the student for the purposes of accessing or communicating in electronic systems as long as that information alone cannot be used to access protected educational records; participation in district-sponsored or district-recognized activities and sports; weight and height of members of athletic teams; dates of attendance; degrees, honors and awards received; artwork or course work displayed by the district;

    - schools or school districts previously attended; and photographs, videotapes, digital images and recorded sound unless such records would be considered harmful or an invasion of privacy
- Limited Directory Information
    - Student's address, telephone number and e-mail address and the parents' addresses, telephone numbers and e-mail addresses
    - This information may only be disclosed as permitted in Board Policy 2400.

Public Information

Public Information has been specifically approved for public release by the Director of Communications or appropriate district administrator. Examples of public information may include patron mailings and materials posted to the district’s website.
This information may be disclosed outside of the district.

Appendix E

Securing Data at Rest and Transit

All staff and students that log into a district provided computer will be provided with several options for data storage and transmission. Staff and students will need to ensure that they are securely storing their data. Staff and students will be able to store data on their local device. It is important to note that this data is not a part of the district's continuity plan, and thus will not be backed up by the district's backup solution. Staff and students may also have a mapped folder. These folders act as folders to district file servers. Access to these files is restricted to the folder's owner (staff or student who is assigned) and district enterprise administrator accounts.

Cloud Storage and File Sharing

The term "Cloud Storage" is used to define all types of remote server storages accessed by users through the internet. All staff and students are provided with a G Suite for Education account that provides unlimited storage. Users are responsible for all digital content on their district provided G Suite for Education Drive.

When using cloud storage, staff must adhere to the following guidelines:

- Staff and students may not access cloud storage through third party applications outside of approved internet browsers and Google Drive App on Android & iOS. This will ensure that native operating systems do not replace cloud sharing security.
- When exiting the district, students should responsibly copy their content to their own personal storage solution.
- When exiting the district, staff should ensure that they are only copying personal content that they created.
- Staff are prohibited from copying content that contains confidential information, student
- records, files, or data.
- Data with personally identifiable information of staff or students may be posted to users' district provided Google Drive with appropriate security settings. Users may not post this data to other cloud sharing platforms without consent of district administration.
- All users shall immediately report any cloud storage security problems of the district's technology resources to a teacher or administrator.
- Attempting to gain or gaining unauthorized access to cloud storage or the files of another is prohibited.
- As with other forms of district technology, district employees, students, and other Google Apps for Education drive users have no expectation of privacy on data stored on this platform.

The term "File Sharing" is used to define all activities sharing access to digital information whether on the cloud or district administered mapped drives. When file sharing, staff must adhere to the following guidelines:

- Users must abide by all policies and procedures regarding professional conduct and communication when sharing, reviewing, updating, commenting and re-sharing.
- When sharing content, users must ensure that other users accessing the information in the files have appropriate access to the information based on job function.

- All users shall immediately report any inappropriate sharing of the district's technology resources to an administrator.

External Storage Devices

The term "External Storage Devices" is used to define all portable storage devices (including USB drives, rewritable CD/DVD, memory cards, and external hard drives) used by staff and students. While the district recognizes the advantages for staff and students to maintain information on these devices, users are strongly encouraged to rely on their district provided Google Apps for Education Drive account for all storage needs.

When using external storage devices, staff must adhere to the following guidelines:

- Users are responsible for all content on external storage devices that have been connected to district technology resources.
- Users must ensure that they will not introduce harmful software including computer viruses, malware, non-district approved software, or hacking tools to district technology resources.
- Users must ensure that the data will remain secure through appropriate encryption or password protection when transferring files containing PII or protected information to an external storage device.

Appendix F

Physical Security Controls

The following physical security controls shall be adhered to:

- Monitor and maintain data centers' temperature and humidity levels. The American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE) recommends an inlet temperature range of 68 to 77 degrees and relative humidity of 40% to 55%.
- File servers and/or storage containing PII, Confidential and/or Internal Information shall be installed in a secure area to prevent theft, destruction, or access by unauthorized individuals.
- Ensure network systems and network equipment are properly secured to prevent unauthorized physical access and data is properly safeguarded to protect from loss.
- Computers and other systems shall be secured against use by unauthorized individuals. It is the responsibility of the user to not leave these devices logged in, unattended, and open to unauthorized use.
- Monitor and control the delivery and removal of all asset-tagged and/or data-storing technological equipment or systems.
- When staff leave the district, they must ensure that they delete any district files, or data from their personal external storage devices.

File Transmission Practices

- Staff are responsible for securing sensitive data for transmission through email or other channels with encryption or a password.
- Staff should never include a password in any communication with the actual file attached that is being protected by the password.
- Staff should never transmit files labeled classified, confidential, or restricted through email or third party file transfer services without district approval.
- Regular transmission of student data to services such as a learning management system is managed by the technology department using a secure data transfer protocol.

All such services are approved by a district/building administrator and the Director of Instructional Technology.

Appendix G

Asset Management

Data security must be maintained through the life of an asset, including the destruction of data and disposal of assets. Any computer, laptop, mobile device, printing and/or scanning device, network appliance/equipment, AV equipment, server, internal or external storage, communication device or any other current or future electronic or technological device may be referred to as a system, asset or device.

All involved systems and information are assets of the district and are expected to be protected from misuse, unauthorized manipulation, and destruction.

Inventory

All devices or systems considered an asset are inventoried. This includes, but is not limited to, network appliances, servers, computers, laptops, mobile devices, and external hard drives.

Disposal Guidelines

Assets shall be considered for disposal in accordance to state/federal regulations and Board policy.

The following considerations are used when assessing an asset for disposal:

- End of useful life
- Lack of continued need
- Obsolescence
- Wear, damage, or deterioration
- Excessive cost of maintenance or repair

The Director of Instructional Technology shall approve disposals of any district technology asset.

Methods of Disposal

Once equipment has been designated and approved for disposal, it shall be handled according to the following methods.

Salvage

All technology assets shall be salvaged in a manner consistent with applicable environmental regulations. Electronic equipment may contain hazardous materials such as mercury, lead, and hexavalent chromium. In addition, systems may contain Personally Identifiable Information (PII), Confidential, or Internal Information. A district-approved vendor shall be contracted for the disposal of all technological systems/equipment. The vendor shall provide written documentation verifying the method used for disposal and a certificate stating that no data of any kind can be retrieved from the hard drive or any other component capable of storing data. Under no circumstances should any technological systems/equipment be placed in the trash.

Appendix H

Virus, Malware, Spyware, Phishing and SPAM Protection

Virus, Malware, and Spyware Protection

SSD desktops, laptops, and file servers are protected using enterprise virus/malware/spyware software. Definitions are updated weekly and an on-access scan is performed on all “read” files continuously. A full scheduled scan runs weekly. A full scheduled scan is performed on all servers weekly during non-peak hours. All files and systems are scanned.

Internet Filtering

Student learning using online content and social collaboration continues to increase. Sedalia Schools views Internet filtering as a way to balance safety with learning—letting good content, resources, and connections in while blocking the bad. To balance educational Internet resource and application use with student safety and network security, the Internet traffic from all devices on the district network is routed through the district firewall and content filter.

All personal devices are required to authenticate prior to gaining access to the district network. This process sets the filtering level appropriately based on the role of the guest user. All sites that are known for malicious software, phishing, spyware, etc. are blocked.

Phishing and SPAM Protection

Email is filtered for viruses, phishing, spam, and spoofing using Google services.

Security Patches

Servers patch management is performed at regular intervals. Security patches are applied on an as needed basis, but at least quarterly.

Appendix I

Account Management

Access controls are essential for data security and integrity. Sedalia Schools maintains a strict process for the creation and termination of district accounts. All new employee accounts are authorized through an HR hiring process prior to creation. Role-based permissions are used to establish access to all systems. Access security is audited at least annually or whenever access permission requirements are changed for a particular application/software or when an application/software is no longer necessary.

Employee Accounts

When an employee is hired by the Sedalia 200 School District, the following process ensures that each staff member has the correct access and permissions to the resources that are required for their position.

- Notification of new employee is sent from Human Resources to the Technology Department. This notification includes position, building assignment(s), and start date.
- Only after notification has been received from Human Resources, the Technology Department creates user accounts. The user is given access and permissions to the necessary resources based on their position and building assignment(s) (see Appendix J: Data Access Roles and Permissions).

When a staff member's employment is ended, either by termination or resignation, account permissions are revoked in one of two ways.

- In the event of termination, HR will send immediate notification via email or phone call to Technology leadership requiring the account to be disabled at once, preventing any further access to district resources. HR will also send a Suspension of Service showing the termination date.
- In the event of resignation, HR sends a Suspension of Service to Technology, indicating the termination date. The account is disabled at the end of business on the termination date, preventing further access to district resources.
- In the event that a user having elevated permissions to any system separates from the district, additional measures are taken to ensure that all elevated accounts to those systems are secure.

Local/Domain Administrator Access

PII, confidential information and/or Internal Information that is stored or accessed remotely shall maintain the same level of protections as information stored and accessed within District's network. In the event that remote access is needed by a contractor/vendor, access must be approved by the Director of Technology. The Assistant Director of Technology Operations or the Network System Administrator will establish the contractor account, only granting access to the server/application that the contractor/vendor supports.

Contractors/Vendors

All contractor/vendor access must be approved by the superintendent of technology. All contractors doing business on district premise must also pass a background check unless other security measures are addressed in a vendor contract. All contractors/vendors accessing district data will be considered on premise users. Once the approval has been obtained, the technology department will create the account.

Appendix J
Data Access Roles and Permissions

Student Information System (SIS)

All staff members are entered into the SIS system. However, only staff requiring access are provided accounts for the system.

The following information is entered for each staff member:

- Start Date
- Building/Site location
- End Date (if applicable)
- Position(s)/Job Duty
- Active
- Separation of Service (SOS)

After basic information and user ID are created then site(s) are applied to account and permissions are given.

Employee permissions are only extended to the site(s) that are assigned to the account.

Permissions (unless employee needs additional permissions) are based on job title and lines up with the names of permissions and are distinguished between Site and District.

Permissions are based on Past, Current, and Future years per individual permission.

- Teacher > Teacher
- Principal > Site Administrator
- SpEd> SpEd Teacher or SpEd case manager or SpEd Director
- Nurse > Site Nurse

Permissions are preset configured by the system, but permissions may be extended per individual basis based on special needs and/or multiple positions being covered by a single account. These changes must be approved by site administrator and/or HR.

Student Information Access

- Attendance being type of attendance and in/out time to the minute
  - View: Site Administrators, Counselors, Teachers, Secretaries, Nurses, and Social Workers.
  - Maintain: Site Secretary, and SIS administrator.
- Grades/Assessments including everything in the gradebook Assignments, Tests, Finals, etc.
  - View: Counselors, Site Administrators
  - Maintain: Site Secretaries, Teachers, SIS administrator.
- Programs and Services tracks many items including Waivers, 504s, SpEd (notes for Sped track), ELL, ESL, etc.
  - View: Anyone with access to search for student can see the icons at the top
  - Maintain: Specific to department_ SpEd > SpEd track import Building administrators
- Discipline
  - View: Counselors, SPED
  - Maintain: Site Administrators, Secretaries, SIS administrator
- Parent Communication (Email, Phone numbers, addresses)
  - View: Teachers, Site Administrators, Counselors, Librarian, Nurses, and Social Workers.

    - Maintain: Secretaries
- Family Demographics
    - View: Secretaries, Site Administrators, Teachers, Nurses, Social Workers, and Counselors.
    - Maintain: District Administrators, Secretaries.
- Fees
    - View: Site Administrators, Counselors, Librarians, and Social Workers.
    - Maintain: Secretaries
- Medical Information
    - Medical data includes Immunizations, Conditions, Medications, and Clinic Logs (Time in/out of clinic and action taken).
    - Site Administrators and Site nurses and Secretaries are the only accounts that can VIEW ALL medical information.
    - Site Nurses are the ONLY accounts that can MAINTAIN medical information.
    - Accounts that can view medications, conditions, immunizations are District SpEd Director, Site
    - Administrator, Site Nurse, Site SpEd Case manager.
    - Site Secretaries can view conditions and immunizations.
    - Counselors view clinic logs and immunizations.

SIS Permission Groups

- B&G Club
- Coaches
- District Administrator
- District Food Service Director
- District Secretary
- District SISK12 Administrator
- District SPED Director
- Juvenile
- Site Administrator
- Site Counselor
- Site Food Service POS Cashier
- Site Librarian
- Site Nurse
- Site Secretary
- Site SpEd Coordinator
- Site SpEd Case Manager/Service Provider
- Site Sub Teacher (Long Term)
- Teacher
- Upward Bound
- View Only

Financial System

All staff members are entered into the financial system for the purpose of employee payroll and HR tracking. Employee access to their individual payroll information is granted through the employee portal. Only staff requiring access are provided accounts for the financial/personnel application. After basic information and user ID are created then permissions are given according to position.

Special Education System

Our special education system houses student IEP information. New accounts are imported at the beginning of the school year and added and adjusted manually throughout the year by the SIS administrator.
Information of staff member including:
Start Date

- Building/Site location
- End Date (if applicable)
- Position(s)/Job Duty
- Work status: Active, Transfer, Separation of Service (SOS)

After basic information and user ID are created then permissions are given according to position:

- SpEd District Administrator
- SpEd Building Coordinator
- SpEd Teacher
- Principal- view only for building

Special Education Administrators have access to all students in the district.

Appendix K

Password Security

The District requires the use of strictly controlled passwords for network access and for access to secure sites and information.
All passwords to district systems shall meet or exceed the below requirements.

- Passwords shall never be shared with another person.
- Every password shall, where possible, be changed at least once per semester.
- When possible, user created passwords should adhere to the same criteria as required for district network access as outlined below.
- Passwords shall not be recorded anywhere that someone may find and use them.

District network access to resources managed through Active Directory/SSO:
Passwords must meet the following complexity requirements:

- At least eight (8) characters in length
- You will not be allowed to use your previous password.
- Passwords must be reset at least once per semester

Where possible, system software should enforce the following password standards:

- Passwords shall be entered in a non-display field.
- System software shall disable the user password when more than five consecutive invalid passwords are given. Lockout time shall be set at a minimum of 10 minutes.

Appendix L

Technology Disaster Response Plan

Objectives

The primary purpose of the Technology Disaster Recovery Plan is to enable Sedalia Schools to respond effectively and efficiently to a natural disaster or critical failure of the district's data center and/or core systems. The objectives during a natural disaster or critical failure are the following:

- Minimize the loss or downtime of core systems and access to business critical data.
- Recover and restore the district's critical systems and data.
- Maintain essential technology resources critical to the day to day operations of the district.
- Minimize the impact to the staff and students during or after a critical failure.

Planning Assumptions

The following planning assumptions were used in the development of Sedalia School District Technology Data Breach Plan:

- There may be natural disasters that will have greater impact than others.
- There will be factors that are beyond the department's control or ability to predict during a disaster.
- There is the possibility of complete loss of the current data center.
- We will have adequate storage to recover systems.0
- District data is housed at district data center and backed up off-site
- District data is hosted by 3rd party providers.
- In the event of a critical failure to network infrastructure in the datacenter, District networking may be significantly impacted.

Disaster Recovery/Critical Failure Team

Sedalia School District has appointed the following people to the disaster recovery/critical failure team: Superintendent over Technology and designees.

In the event the Technology Disaster Recovery Plan is activated, overall management of the response is delegated to this team.

Their primary responsibilities include:

- Determining the impact of the natural disaster/critical failure.
- Communication of impact and or loss, and updates of progress to the District Superintendent.
- Communication of outages and updates to district staff.
- Oversight of the Technology Disaster Recovery Plan implementation and restoration of critical systems and data.
- Allocation and management of technology staff during the event.
- Working with manufacturers and/or vendors during the recovery and restoration of critical systems and data.
- Oversight of Technology Disaster Recovery Plan implementation debrief.

Activation

The Technology Disaster Recovery Plan will be activated in the event of the following:

- A natural disaster has occurred and affects the operation of the District's data center. A natural disaster includes but is not limited to the following: tornado, earthquake, lightning, and flood.
- A fire has impacted the data center.
- Water or flooding has impacted the data center.
- Critical system failure.

The Director of Technology will act as the incident response manager. If the Information Security Officer is not able to act as the incident response manager, a member of the Superintendent's Leadership Team will assume the role of incident response manager, with assistance from the Incident Response Team.

Notification

The following groups will be notified as needed in the event the plan has been activated:

- Superintendent
- Superintendent's Leadership Team (SLT)
- Technology Staff
- District Employees
- Parents and Students
- Vendors

Information will be disseminated to the above groups through whichever means of communication is available at the time.

This could include any one or combination of the following:

- Phone
- Email
- Social Media
- Radio or Television

The Technology Disaster Recovery Plan team will work with district leadership, including the Director of Communications, on which information will be conveyed to each above group and what means will be used.

Implementation

The Technology Disaster Recovery Plan team has the following in place to bring the District back online in the least of amount of time possible:

Maintained spreadsheet listing all server names (servers.xlsx), physical and virtual, and their function.

- A copy of this document will be secured on a district server. An electronic version will be housed on Google Drive.
- Maintained spreadsheet of, needed passwords and vendor contact information.
- A copy of this document will be secured on a district server. An electronic version will be housed on Google Drive.
- The District's data backup solution includes the use of a third-party vendor, which backs up data locally in the datacenter.
- In the event of a critical system failure, the District can restore that server back to our current environment from the backup solution.

Evaluation

An internal evaluation of Sedalia School District Technology Disaster Recovery Plan response will be conducted. This will entail gathering documentation from the response and feedback from all stakeholders and incorporate into an after action report and corrective action plan. The result will be an update to the Technology Disaster Recovery Plan and other emergency response plans as appropriate.

Appendix M

Data Breach Response Plan

Objectives

The purpose of the Technology Data Breach Plan is to enable the Sedalia School District to respond effectively and efficiently to an actual or suspected data breach involving personally identifiable information (PII), confidential or protected information, district identifiable information and other significant cybersecurity incident.

The objectives of the Technology Data Breach Plan are:

- Convene the Incident Response Team as necessary.
- Validate and contain the data security breach.
- Analyze the breach to determine scope and composition.
- Minimize impact to the staff and students after a data breach has occurred.
- Notification of data owners, state/federal agencies and law enforcement as deemed necessary.

Planning Assumptions

The following planning assumptions were used in the development of Sedalia School District Technology Data Breach Plan:

- There may be data breaches that will have greater impact than others.
- There will be factors that are beyond the department's control or ability to predict during a data breach.
- District data is backed up off site.
- District data is hosted by 3rd party providers.

Data Breach/Incident Response Team

Sedalia School District has appointed the following people to the data breach/incident response team: Superintendent of Technology, Director of Technology, Network Administrator, and 3rd party hosting vendors as needed.

In the event the Technology Data Breach Plan is activated, overall management of the response is delegated to this team. Their primary responsibilities include:

- Determine the nature of the data compromised and its impact to staff, students and the district itself.
- Communicate impact, the number of affected individuals, the likelihood information will be or has been used by unauthorized individuals and updates of progress to the District Superintendent and Superintendent of Technology.
- Coordinate with Director of Communications to ensure communication with district staff and or parents as deemed appropriate.
- Oversight of the Technology Data Breach Plan implementation and data breach resolution.
- Allocate and manage technology staff resources during the event.
- Work with vendors, 3rd party providers, manufacturers, state/federal agencies and law enforcement while correcting the data breach and its repercussions.
- Oversight of Technology Data Breach Plan implementation debrief.

Activation

The Technology Data Breach Plan will be activated in the event of the following:

- A data breach has occurred and affects the district itself.
- A data breach includes but is not limited to an incident in which sensitive, protected or confidential data has potentially been viewed, stolen or used by an individual unauthorized to do so.
- Personal Health Information (PHI) has been compromised.
- Personally Identifiable Information (PII) has been compromised.
- Confidential or sensitive data has been compromised.
- Network hack/intrusion has occurred.

The Information Security Officer will act as the incident response manager. If the Incident Security Officer is not able to act as the incident response manager, a member of the Superintendent's Leadership Team will assume the role of incident response manager, with assistance from the Incident Response Team. The breach response and reporting process will be documented. The Superintendent of Technology will work with the Director of Communications to dispense and coordinate the notification and public message of the breach.

Notification

The following groups will be notified as needed in the event the plan has been activated:

- Superintendent
- Superintendent's Leadership Team
- Technology Staff
- District Employees
- Parents and Students
- Vendors

Information will be disseminated to the above groups through whichever means of communication deemed appropriate.

This could include any one or combination of the following:

- Email
- Social Media
- Radio or Television
- First Class Mail
- Phone

The Technology Data Breach Plan team will work with district leadership on which information will be conveyed to each above group, timing of that communication and what means will be used.

Implementation

The Technology Data Breach Plan team has the following in processes in place to contain the data breach in the least amount of time possible:

- Data inventory of all systems containing sensitive data. A copy of this document will be secured on a district server. An electronic version will be housed on Google Drive.
- Maintained spreadsheet listing all server names (servers.xlsx), physical and virtual, and their function. A copy of this document will be secured on a district server. An electronic version will be housed on Google Drive.
- The District's data backup solution includes the use of a third-party vendor which backs up data locally in the datacenter.

- The following will take place during the incident response:
- The members of the Incident Response Team will be assembled once a breach has been validated. The Incident Response Team will be comprised of the Director of Technology, Information Security Officer, Network Administrator. Additional members of the Sedalia School District administrative team and technology department may be designated to assist on the Incident Response Team.
- The Incident Response Team will determine the status of the breach, on-going, active, or post-breach.
- For an active and ongoing breach, the Incident Response Team will initiate appropriate measures to prevent further data loss.
- These measures include, but are not limited to, securing and blocking unauthorized access to systems/data and preserving any and all evidence for investigation.

- The Incident Response Team will work with the data managers and data owners to determine the scope and composition of the breach, secure sensitive data, mitigate the damage that may arise from the breach and determine the root cause(s) of the breach to devise mitigating strategies and prevent future occurrences.
- The incident response manager will work with legal counsel and the Superintendent of Technology to determine appropriate course of action pursuant to state statute. This includes notification of the authorities, local law enforcement, and the Missouri State Attorney General.
- Collaboration between the authorities and the Incident Response Team will take place with the incident response manager.
- The IRT will work with the proper authorities to make sure any and all evidence is properly handled and preserved.
- On advice from legal counsel, an outside party may be hired to conduct the forensic investigation of the breach.
- When the investigation has concluded, all evidence will be safely stored, recorded or destroyed
- (where appropriate).
- All affected data, machines and devices will be identified and removed from the network as deemed appropriate for the investigation.
- Interviews will be conducted with key personnel and facts of the incident will be documented and the evidence preserved for later examination.
- The Incident Response Team will work with the Sedalia School District Communications department to outline the notification of the data owners and those affected.
- Communication will be sent out as directed by legal counsel and advised by the district communications team. The types of communication will include, but not limited to, email, text message, postal mail, substitute notice and/or phone call.
- Once the incident response team has determined the severity of the breach, the team will notify the Incident Response Manager to determine whether or not the Family Policy Compliance Office (FPCO) or PTAC needs to be notified.
- The Incident Response Manager, in conjunction with the Incident Response Team, legal counsel and the Superintendent's Leadership Team will determine if the notification of affected individuals is necessary. Once the determination is made to notify affected individuals, a letter will be written in accordance with all federal and state statutes.

Evaluation

Once the breach has been mitigated an internal evaluation of SSD Technology Data Breach Plan response will be conducted. The IRT, in conjunction with the incident response manager and others that were involved, will review the breach and all mitigation steps to determine the probable cause(s) and minimize the risk of a future occurrence. Feedback from the responders and affected entities will be incorporated into an after action report and corrective action plan. The result will be an update to the Technology Data Breach Plan and other emergency response plans as appropriate. Information security training programs will be modified to include countermeasures to mitigate and remediate previous breaches so that past breaches do not recur. The reports and incident review will be filed with all evidence of the breach.