Data Governance Manual
# Contents

- Introduction ............................................................................................................................................................................. 4
  - Data Governance Team .......................................................................................................................................................... 4
  - Purpose ..................................................................................................................................................................................... 4
  - Scope .......................................................................................................................................................................................... 5
  - Regulatory Compliance ............................................................................................................................................................ 5
  - Data User Compliance ............................................................................................................................................................. 6

- Data Lifecycle ............................................................................................................................................................................. 8
  - Identifying Need & Assessing Systems for District Requirements ......................................................................................... 8
    - New Systems ........................................................................................................................................................................... 8
    - Review of Existing Systems ................................................................................................................................................. 9
  - Acquisition and Creation ........................................................................................................................................................ 11
  - Management and Storage ......................................................................................................................................................... 11
    - Systems Security ................................................................................................................................................................. 11
    - Data Management ............................................................................................................................................................... 12
    - Data Inventory and Classification ....................................................................................................................................... 12
    - Securing Data at Rest and Transit .................................................................................................................................... 13
  - Security/Protection .................................................................................................................................................................. 13
    - Risk Management ................................................................................................................................................................. 13
    - Security Logs .......................................................................................................................................................................... 13
    - Logon Banners ....................................................................................................................................................................... 13
    - Physical Security Controls .................................................................................................................................................... 14
    - Virus, Malware, Spyware, Phishing and SPAM Protection ................................................................................................... 14
    - Electronic Access Security Controls .................................................................................................................................... 14
    - Securing Data at Rest and Transit ....................................................................................................................................... 16
  - Usage and Dissemination ......................................................................................................................................................... 16
    - Securing Data at Rest and Transit ....................................................................................................................................... 16
    - Training ................................................................................................................................................................................... 18
  - Archival and Destruction .......................................................................................................................................................... 18
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>District Data Destruction Processes</td>
<td>18</td>
</tr>
<tr>
<td>Asset Disposal</td>
<td>18</td>
</tr>
<tr>
<td>Critical Incident Response</td>
<td>19</td>
</tr>
<tr>
<td>Business Continuity</td>
<td>19</td>
</tr>
<tr>
<td>Disaster Recovery</td>
<td>19</td>
</tr>
<tr>
<td>Data Breach Response</td>
<td>19</td>
</tr>
<tr>
<td>Appendix A Definitions</td>
<td>20</td>
</tr>
<tr>
<td>Appendix B Laws, Statutory, and Regulatory Security Requirements</td>
<td>22</td>
</tr>
<tr>
<td>Appendix C Digital Resource Acquisition and Use</td>
<td>24</td>
</tr>
<tr>
<td>Appendix D Data Security Checklist</td>
<td>26</td>
</tr>
<tr>
<td>Appendix E Data Classification Levels</td>
<td>27</td>
</tr>
<tr>
<td>Appendix F Securing Data at Rest and Transit</td>
<td>29</td>
</tr>
<tr>
<td>Appendix G Physical Security Controls</td>
<td>32</td>
</tr>
<tr>
<td>Appendix H Asset Management</td>
<td>33</td>
</tr>
<tr>
<td>Appendix I Virus, Malware, Spyware, Phishing and SPAM Protection</td>
<td>35</td>
</tr>
<tr>
<td>Appendix J Account Management</td>
<td>36</td>
</tr>
<tr>
<td>Appendix K Data Access Roles and Permissions</td>
<td>38</td>
</tr>
<tr>
<td>Appendix L Password Security</td>
<td>41</td>
</tr>
<tr>
<td>Appendix M Technology Disaster Recovery Plan</td>
<td>42</td>
</tr>
<tr>
<td>Appendix N Data Breach Response Plan</td>
<td>45</td>
</tr>
</tbody>
</table>
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 RQS 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 RQS Data Governance Policy 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.

Data Governance Team

The RQS Data Governance team consists of the following positions: Superintendent, Associate Superintendent of Curriculum and Instruction, Associate Superintendent of Operations, Assistant Superintendents of Elementary and Secondary Education, Assistant Superintendent of Human Resources, Chief Communications Officer, and Chief Information Officer. Members of the Data Governance Team will act as data stewards for all data under their direction. The Chief Information Officer (CIO) will act as the Information Security Officer (ISO), with assistance from the Assistant Directors of Technology. The Assistant Director of Technology Operations is the district’s alternate ISO and will assume the responsibilities of the ISO when the ISO is not available. All members of the district administrative team will serve in an advisory capacity as needed.

Purpose

Raytown Quality Schools’ technology exists for the purpose of enhancing the educational opportunities and achievement of district students. Research shows that students who have access to technology improve achievement. Technology assists with the professional enrichment of the staff and increases engagement of students’ families and other patrons of the district, all of which positively impact student achievement.

To accomplish the district’s mission and comply with the law, the district must collect, create and store confidential 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.

It is the policy of Raytown Quality 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. All employees and authorized district contractors or agents using confidential 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 Raytown Quality 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 considered assets of Raytown Quality Schools and 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). Raytown Quality 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)
- Payment Card Industry Data Security Standard (PCI DSS)
- 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 Raytown Quality 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 EHBC (Data Governance and Security), EHB (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.

Unless permission has been granted by the ISO or designee, 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.

Employees who fail to follow the law or district policies or procedures regarding data governance and security may be disciplined or terminated. Students may be suspended or expelled. 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.

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 (exception for authorized technology staff for the purpose of support)
- Applying for a user ID under false pretenses or using another person’s ID or password.
- Unauthorized use of an authorized password to invade student or employee privacy by examining records or information for which there has been no request for review.
- The unauthorized copying of system files.
• Attempting to secure a higher level of privilege without authorization.
• Installation or use of unlicensed software or software not approved for district technological systems.
• 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: laptops, 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 maintain confidential information, including information regarding students, parents/guardians, employees, applicants for employment and others. The district will collect, create or store confidential information only when the superintendent or designee determines it is necessary.

New Systems

District staff members are encouraged to research and utilize online services or applications to engage students and further the district’s educational 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.

The Raytown School District has an established process for vetting new resources. Staff are required to complete steps outlined within the Digital Resources flowchart, located in the Staff Technology Handbook, to ensure that all new resources meet business and/or instructional need as well as security requirements.
Memorandums of understanding (MOU) or contracts for any system that create, collect or use personally identifiable information (PII), student records or confidential data must be reviewed by the ISO prior to initiation.

All new resources shall be properly evaluated against the following criteria, when applicable:

- Impact on technology environment including storage and bandwidth
- Hardware requirements, including any additional hardware
- License requirements/structure, number of licenses needed, and renewal cost
- Maintenance agreements including cost
- Resource update and maintenance schedule
- Funding for the initial purchase and continued licenses and maintenance
- Evaluate terms of service, privacy policy, and MOU/contract that meet the following criteria:
  - The district continues to own the data shared, and all data must be available to the district upon request.
  - 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. If metadata is collected, it will be protected to the same extent as the district’s confidential or critical information.
  - District data will be maintained in a secure manner by applying appropriate technical, physical and administrative safeguards to protect the data.
  - 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
  - Student and/or staff data will not be stored on servers outside the US unless otherwise approved by the District.
  - The provider will comply with district guidelines for data transfer or destruction when contractual agreement is terminated.
  - No API will be implemented without full consent of the district.
  - All data will be treated in accordance to federal, state and local regulations
  - The provider assumes liability and provides appropriate notification in the event of a data breach.

Review of Existing Systems

The District will ensure that data collection is aligned with Board Policy EHBC. Data systems shall be regularly reviewed to ensure that only necessary data is being transmitted and collected.

Individual student level data is submitted to different approved service providers in order to ensure business operations and instructional services. At times, these imports include PII for staff and student. The District must ensure that each piece of PII is necessary for operations or instruction and that the providers are abiding by their terms of service.
The District will audit all data imports annually. These audits will include:

- Review of provider’s terms of service to ensure they meet the District’s data security requirements.
- Review of provider’s contract to ensure that all terms are met.
- Verification that software imports are accurate and pulling correct information.
- Verification that, when applicable, the staff, students and classes included in the imports are still necessary for instructional purposes (only those that need data collected are included in import).
- Determine if the fields included in the imports are still necessary for intended purpose.
**Acquisition and Creation**

After completing the requirements for new systems in the above section, Identifying Need & Assessing System for District Requirements, staff shall complete a software request (located online under staff technology resources) for any new digital resources that either has an associated cost or collects staff or student data (see Appendix C: Digital Resource Acquisition and Use). All staff must adhere to the following guidelines regarding digital resource acquisition:

- Contracts for any system that creates, collects or uses personally identifiable information (PII), student records or confidential data must be reviewed by the ISO prior to initiation.
- It is the responsibility of staff to ensure that all electronic resources are age appropriate, FERPA compliant, and are in compliance with software agreements before requesting use.
- It is the responsibility of the staff requesting digital content to properly vet the resource to ensure that it meets district business objectives, is in line with curriculum or behavioral standards, is instructionally sound, and is appropriate for the intended use.
- Digital resources that accompany adopted instructional materials will be vetted by the appropriate Assistant Superintendent and the Chief Information Officer, or designee, prior to purchase.

Prior to initiating services and/or transmitting any data, the district will conduct a risk management audit using the data security checklist (see Appendix D: Data Security Checklist). The data manager will ensure the following:

- System account creation procedures and data access guidelines appropriately match employee job function with the data on instructional and operational systems.
- Proper procedures and practices are in place to ensure accuracy and security of data.
- All staff responsible for use and/or management of the system are trained on data security and integrity.
- All employees with custom data access beyond their typical group’s access are reviewed and need established prior to account creation.

**Management and Storage**

**Systems Security**

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 (BOE Policy EHBC). 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.
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.

Data Managers are responsible for the development and execution of practices and procedures that ensure the accuracy and security of data in an effective manner. 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. Data managers will:

- ensure that system account creation procedures and data access guidelines appropriately match employee job function with the data on instructional and operational systems.
- review all employees with custom data access beyond their typical group’s access.
- annually review district processes to ensure that data will be tracked accurately.
- annually review contracts with instructional and operational software providers to ensure that they are current and meet the district data security guidelines.
- ensure that staff are trained in the district’s proper procedure and practices in order to ensure accuracy and security of data.
- assist the ISO in enforcing district policies and procedures regarding data management.

Data Inventory and Classification

The ISO or designee will identify all systems containing district data, such as student information systems, financial systems, payroll systems, transportation systems, food-service systems, email 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 or designee 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.

Classification is used to promote proper controls for safeguarding the confidentiality of data. Regardless of classification, the integrity and accuracy of all classifications of data are protected. The classification assigned and the related controls applied are dependent on the sensitivity of the data. Data is classified according to the most sensitive detail they include. Data recorded in several formats (e.g., source document, electronic record, report) have the same classification regardless of format (see Appendix E: Data Classification Levels).

Once the data is classified, the ISO or designee will create a data inventory. The ISO or designee will maintain the district’s data inventory in both electronic and printed form and will update it annually. When possible, a data dictionary will be maintained for critical information systems.
The data inventory will contain the following:

- Data Source
- What data is stored: identification of every data field
- Where the data is stored
- Persons assigned to manage the data
- Employees or employee categories that have access to the files
- When the data is collected and received
- How the data is accessed
- Who has access
- Criticality/Sensitivity Rating

**Securing Data at Rest and Transit**

District data security applies to all forms of data, including data stored on devices or on additional resources, such as cloud storage. All district external hard drives will be maintained in inventory and verified through the regular inventory verification process.

Users must ensure that they are securely storing their data. Guidelines have been established for cloud storage and file sharing, external storage devices, and file transmission practices. These guidelines can be found in the Usage and Dissemination section below (see Appendix F: Securing Data at Rest and Transit).

**Security/Protection**

**Risk Management**

A thorough risk analysis of all RQS data networks, systems, policies, and procedures shall be conducted on an annual basis or as requested by the Superintendent, ISO or designee. This analysis shall be completed using the risk management steps outlined in the Data Security Checklist. The product of the risk analysis will be referred to as the risk assessment. The risk assessment shall be used to develop a plan to mitigate identified threats and risk to an acceptable level by reducing the extent of vulnerabilities (see Appendix D: Data Security Checklist).

**Security Logs**

The District will maintain a comprehensive list of critical system events that will be logged and monitored to ensure data security. These events will include, but are not limited to, access to critical systems and modification of critical data. When applicable, notifications will be established for critical event triggers.

**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
Technology telecommunication closets are housed in secure locations. Access authorization is assigned through the Chief Information Officer (BOE Policy ECA-AP1). In addition, access to areas in which information processing is carried out shall be restricted to only appropriately authorized individuals (see appendix G: Physical Security Controls).

No technological systems shall be disposed of or moved without adhering to the appropriate procedures (see Appendix H: 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 H: 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 EHBC). 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.

No user will be granted local administrator permissions unless required for the use of a specific software/application. If at all possible, technology staff will create custom scripts for these programs to run without the users having elevated permissions. In the event that a script cannot eliminate the need for elevated permissions, users may be made local machine administrators. All accounts needing this elevated permission must be approved by the ISO. Once the elevated permissions are no longer required for the
software/application, the technology team will complete an audit of all user accounts and reinstate regular permissions.

Additionally, no users will have domain administrative access. Technicians requiring domain or local machine admin access will have a separate account for the sole purpose of this access. Technicians will use their regular district login (without elevated privileges) for all access not requiring elevated permissions.

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 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 K: Data Access Roles and Permissions). If an employee requires additional access, an Additional Access Request form must be completed and approved by the appropriate data manager and Chief Information Officer.

**Contractors/Vendors**

Access to contractors/vendors is governed through the same process using Board of Education policy EHB-AP1 and EHB-AF4 (External User Technology Agreement). All contractor/vendor access must be approved by HR and ISO. 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, 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. Secure password requirements will be set according to NIST recommended standards (see Appendix L: Password Security). When possible, the district will utilize Single Sign On (SSO) or Active Directory Integration to maintain optimal account security controls.

**Concurrent Sessions**

When possible, the district will limit the number of concurrent sessions for a user account in a system.

**Remote Access**

Access into the District’s network from outside is strictly prohibited without explicit authorization from the ISO. Remote access will be granted through virtual private network (VPN) connection through the district’s network VPN appliance; no other method of remote access shall be granted 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 VPN access is needed by a contractor/vendor, access must be approved by the ISO. 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.

All VPN accounts will be reviewed at least annually.

**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. All district external hard drives will be maintained in inventory and verified through the regular inventory verification process. 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 F: 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 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, maintaining information in locked rooms or drawers, 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 (BOE Policy EHBC).

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 (EHB, EHB-AP1), Data Governance and Security (EHBC, EHBC: AP1, AP2, AP3, AP4 and AP5), Staff Conduct (GBCB, GBCC, GBCC-AP1), and Student Record (JO, JO-AP1).

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.

**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 personal folder. This folder acts as a redirection of document and desktop 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 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 F: 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 redact 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 F: Securing Data at Rest and Transit).

Credit Card and Electronic Payment

Users of systems that process electronic payments, including but not limited to processing credit card information, must adhere to strict guidelines regarding the protection of payment information and cardholder data. These users are responsible for adhering to the appropriate level of PCI compliance when handling such data (see Appendix F: 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 EHBC-AP5. 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 redact 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. This program will consist of the following:

- Training for all new staff on technology policies and procedures, including confidentiality and data privacy.
- Additional training for new instructional staff on federal regulations and the use of digital resources and student electronic records.
- Annual training for all staff on technology policies and procedures, including confidentiality and data privacy.
- Annual training for all instructional staff on federal regulations and the use of digital resources and student electronic records.
- Annual training for district administration on federal regulations, data privacy and security.
- All training or professional learning that includes the use of data systems shall include data security.

Archival and Destruction

Once data is no longer needed, the ISO or designee 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 unretrievable. 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.

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 EHBC-AP5, Data Retention and Business Continuity. District data managers will regularly review systems and data to ensure that data that is 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.
- Student home folder data will be maintained for one school year after the student’s final date of attendance.
- Employee home folder data will be maintained via district data back-ups for 90 days after the final work day, unless HR approves for a district administrator to maintain access.

Asset Disposal

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

**Business Continuity**

The District’s administrative procedure EHBC-AP5, Document Retention and Business Continuity, delineates the process for data retention for all district data including backup requirements. The District will maintain systems that provide near-line and off-site data backup. These systems shall allow for the full recovery of critical systems in the event of a disaster. The district will test near-line and off-site backups quarterly.

**Disaster Recovery**

The District’s Technology Disaster Recovery Plan outlines critical staff, responsibilities, and processes in the event of a disaster or critical data loss. The District shall maintain a list of all critical systems and data, including contact information. Technology Disaster Recovery Plan shall include processes that enable the District to continue operations and efficiently restore any loss of data in the event of fire, vandalism, natural disaster, or critical system failure (see Appendix M: Disaster Recovery Plan).

**Data Breach Response**

District Policy EHBC-AP1 Data Governance and Security (Incident and Data Breach Response Plan) addresses state law regarding a 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 N: Data Breach Response Plan).
Appendix A
Definitions

Confidentiality: Data or information is not made available or disclosed to unauthorized persons.

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: Facts or information. Data can be in any form; oral, written, or electronic.

Data Breach, Breach of Security or Breach: A security incident in which there was unauthorized access to and unauthorized acquisition of personal information maintained in computerized form that compromises the security, confidentiality or integrity of the information.

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 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 ISO 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 development and application owners in the implementation of security controls for information on systems, from the point of system design through testing and production implementation.
**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.

**Security Incident:** An event that 1) actually or potentially jeopardizes the confidentiality, integrity or availability of an information system or the information the system processes, stores or transmits, or 2) constitutes a violation or imminent threat of violation of security policies, security procedures or acceptable-use policies.

**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, MOSIS ID, 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. PII includes but is not limited to (a) student’s name; (b) name of the student’s parent or other family members; (c) address of the student or student’s family; (d) a personal identifier, such as the student’s social security number, student number, or biometric record; and (e) other indirect personal identifiers, such as the student’s date of birth, place of birth, and mother’s maiden name; (f) 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; or (g) “medical information” as may be defined in state law; “protected health information” as that term is defined in the Health Insurance Portability and Accountability Act, 45 CFR Part 160.103; (h) nonpublic personal information as that term is defined in the Gramm-Leach-Bliley Financial Modernization Act of 1999, 15 USC 6809; (i) credit and debit card numbers and/or access codes and other cardholder data and sensitive authentication data as those terms are defined in the Payment Card Industry Data Security Standards; (j) other financial account numbers, access codes, driver’s license numbers; (k) and state- or federal-identification numbers such as passport, visa or state identity card numbers; (l) personal identifiable information as defined by COPPA, including but not limited to online contact information like an email address or other identifier that permits someone to contact a person directly (for example, an IM identifier, VoIP identifier, or video chat identifier), screen name or user name where it functions as online contact information, telephone number, persistent identifier that can be used to recognize a user over time and across different sites (including a cookie number, an IP address, a processor or device serial number, or a unique device identifier), a photo, video, or audio file containing a child’s image or voice, geolocation information sufficient to identify a street name and city or town; or other information about the child or parent that is collected from the child and is combined with one of these identifiers.

**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 ISO 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 cyberbullying 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 (20 U.S.C. § 1232g(a)(4)(A)(ii), 1232g(b)(1)), as amended from time to time applies to all institutions that are recipients of federal aid administered by the Secretary of Education. This regulation protects student information and accords students 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 (PHI). 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 (20 U.S.C. § 1232h; 34 CFR Part 98), 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

- Receive notice and an opportunity to opt a student out of any collection, disclosure, or use of personal information collected from students for marketing or to sell or otherwise distribute the information to others (doesn’t apply if sole purpose is to develop educational products for students or schools).
- 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 Safe Schools Act:** The Missouri Safe Schools Act (Missouri Revised Statutes § 160.261) attempts to standardize the response of school districts across the state to acts of violence committed by students.

**Missouri Sunshine Law:** Missouri law (§ 610.011, RSMo) that states that meetings, records, votes, actions, and deliberations of public governmental bodies be open to the public unless otherwise provided by law.

**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.
Appendix C
Digital Resource Acquisition and Use

The purpose of the Digital Resource Acquisition and Use process is to:
- ensure proper management, legality and security of information systems.
- increase data integration capability and efficiency.
- minimize malicious code that can be inadvertently downloaded.

New Resource Acquisition

Staff are required to complete steps outlined within the Digital Resources flow chart for both instructor and student resources. In addition, a software resource request form (found online under staff technology resources) is required for any new digital resources that either has an associated cost or collects staff or student data. All staff must adhere to the following guidelines regarding digital resource acquisition:
- Contracts for any system that creates, collects or uses personally identifiable information (PII), student records or confidential data must be reviewed by the ISO prior to initiation.
- It is the responsibility of staff to ensure that all electronic resources are age appropriate, FERPA compliant, and are in compliance with software agreements before requesting use.
- It is the responsibility of the staff requesting digital content to properly vet the resource to ensure that it meets district business objectives, is in line with curriculum or behavioral standards, is instructionally sound, and is appropriate for the intended use.
- Digital resources that accompany adopted instructional materials will be vetted by the appropriate Assistant Superintendent and the Chief Information Officer, or designee, prior to purchase.

All new resources shall be properly evaluated against the following criteria, when applicable:
- Impact on technology environment including storage and bandwidth
- Hardware requirements, including any additional hardware
- License requirements/structure, number of licenses needed, and renewal cost
- Maintenance agreements including cost
- Resource update and maintenance schedule
- Funding for the initial purchase and continued licenses and maintenance
- Evaluate terms of service, privacy policy, and MOU/contract that meet the following criteria:
  - Student and/or staff data will not be shared, sold, or mined with or by a third party.
  - Student and/or staff data will not be stored on servers outside the US.
  - The provider will comply with district guidelines for data transfer or destruction when contractual agreement is terminated.
  - No API will be implemented without full consent of the district.
  - All data will be treated in accordance to federal, state and local regulations.
  - The provider assumes liability and provides appropriate notification in the event of a data breach.
Approved Digital Resources

In order to ensure that all resources used meet security guidelines and to prevent software containing malware, viruses, or other security risk, digital resources that have been evaluated are categorized as Approved or Denied. Prior to approval/denial, digital resources shall be approved by the Chief Information Officer or designee.

- A list of evaluated software will be maintained on the District Technology site.
- It is the responsibility of staff to submit requests resources review if a resource is not listed.
- Resources that are labeled denied or have not yet been reviewed will not be allowed on district owned devices or used as part of district business or instructional practices.

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 RQS systems and other electronic devices will have a current license on file or will be removed from the system or device.
- Digital resources that are accessed from and/or that store data in a cloud environment will have a memorandum of understanding (MOU) or contract on file that states or confirms at a minimum that:
  - Student and/or staff data will not be shared, sold, or mined with or by a third party.
  - Student and/or staff data will not be stored on servers outside the US.
  - The provider will comply with district guidelines for data transfer or destruction when contractual agreement is terminated.
  - No API will be implemented without full consent of the district.
  - All data will be treated in accordance to federal, state and local regulations.
  - The provider assumes liability and provides appropriate notification in the event of a data breach.
- 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 Security Checklist

A thorough risk analysis of all RQS data networks, systems, policies, and procedures shall be conducted on an annual basis or as requested by the Superintendent, ISO or designee.

The Data Security Checklists examine the types of threat that may affect the ability to manage and protect the information resource. The analysis also documents any existing vulnerabilities found within each entity, which could potentially expose the information resource to threats. Finally, the analysis includes an evaluation of the information assets and the technology associated with its collection, storage, dissemination and protection.

From the combination of threats, vulnerabilities, and asset values, an estimate of the risks to the confidentiality, integrity and availability of the information is determined. The product of the risk analysis will be referred to as the risk assessment. The risk assessment shall be used to develop a plan to mitigate identified threats and risk to an acceptable level by reducing the extent of vulnerabilities.

Data Security Checklist for District Hosted Systems

- Inventory and classification of data on system
- Types of potential threats (internal, external, natural, manmade, electronic and nonelectronic)
- Physical security of system
- Location within network including network systems protection (firewall, content filter) and if system is externally facing or only allows for district network access
- Access controls including password security (can district password requirements be enforced)
- Authentication methods (Active Directory, Single Sign On, District managed account, user managed account)
- Server/system security patch frequency
- Ability to access from mobile devices
- Ability to maintain critical system event logs
- Ability to receive notification for critical system events

Data Security Checklist for Provider Hosted Systems

- Inventory and classification of data on system
- Types of potential threats (internal, external, natural, manmade, electronic and nonelectronic)
- Contract, terms of service and privacy policy are current and meet district data security requirements
- Provider has adequate data security measures including data management and incident response
- Ability to ensure proper access controls including password security (can district password requirements be enforced)
- Authentication methods (Active Directory, Single Sign On, District managed account, user managed account)
- Server/system security patch frequency
- Ability to access from mobile devices
- Notification practices in the event of a system compromise or security breach
Appendix E
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. Decisions about the provision of access to this information shall always be cleared through the data manager and/or ISO.

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 coursework 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 email address and the parents' addresses, telephone numbers and email addresses

This information may only be disclosed as permitted in Board Policy JO.

**Public Information**

Public Information has been specifically approved for public release by the Chief Communications Officer 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 F

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 personal folder. This folder acts as a redirection of document and desktop 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.

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.

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. Users are responsible for all digital content on their district provided Google Apps 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. An example of an unapproved application would be the Google Drive app on Windows machines.
- Users need to be aware of default sharing settings on folders when they upload files. Users are required to limit sharing files to an as needed basis.
- Staff and students must ensure that any cloud storage providers used are approved by the district and meet district student data and data security standards.
- 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 or district created curricular or operational documentation, 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.
- Staff should never post any documents labeled classified, confidential, or restricted to any cloud storage including district provided Google Drive accounts without district approval.
- 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 that share access to digital information whether in the cloud or on 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. Users should only keep the information stored on the external device for the duration of the project, and then promptly remove.
• Staff should never transfer any documents labeled classified, confidential, or restricted to any external storage device.
• Staff should never transfer or create confidential data or student records on personal storage devices.
• When staff leave the district, they must ensure that they delete any district created/provided curricular or operational documentation, 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 Chief Information Officer.

**Credit Card and Electronic Payment**

Users of systems that process electronic payments, including but not limited to processing credit card information, must adhere to strict guidelines regarding the protection of payment information and cardholder data. These users are responsible for adhering to the following requirements and appropriate level of PCI compliance when handling such data:

- Never store cardholder data on district systems or in written form. All cardholder data may only be entered in secured payment systems approved by the district. Any cardholder data collected in written form must be shredded immediately after entry into approved system.
- The district will never maintain a data system for payment information. All payment information will be stored and processed by a 3rd party accessible through a secure portal.
- Never request cardholder information to be transmitted via email or any other electronic communication system.
- Payment information shall be entered directly into the approved payment system by individual making payment. If the individual is not able to directly input the payment, designated staff may gain verbal approval for the payment process either in person or via phone (after identification is verified). If verbal payment information is received, that information must be entered directly into the payment system and not written down during the process.
- If payment information is collected via a physical form, that form must be shredded or payment information redacted immediately upon receipt and entry into payment system.
Appendix G
Physical Security Controls

The following physical security controls shall be adhered to:

- Network systems shall be installed in an access-controlled area. The area in and around the computer facility shall afford protection against fire, water damage, and other environmental hazards such as power outages and extreme temperature situations.
- 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. A record shall be maintained of all personnel who have authorized access.
- 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. Maintain a record of all such items entering or exiting their assigned location using the district approved technology inventory program. No technology equipment regardless of how purchased or funded shall be moved without the explicit approval of the technology department.
- Ensure that technological equipment or systems being removed for transfer to another organization or being designated as surplus property is appropriately sanitized in accordance with applicable policies and procedures (see Appendix I: Asset Management).
- Monitor and maintain a list of employees with building access and will routinely monitor this list to ensure that only current employees continue to have this access (per BOE Policy ECA & ECA-AP1).
- Monitor and maintain a numbered key card check-out system in order to manage recipients of all key cards distributed (per BOE Policy ECA & ECA-AP1).
Appendix H
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 by the technology department. This includes, but is not limited to, network appliances, servers, computers, laptops, mobile devices, and external hard drives. The technology department will conduct bi-annual inventory verifications of all staff devices and at least an annual inventory verification of student devices. It is the responsibility of the technology department to update the inventory system to reflect any in-school transfers, in-district transfers, or other location changes for district technology assets.

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 Chief Information Officer shall approve disposals of any district technology asset. Documentation of the asset disposal will include the asset tag number, description, serial number and method of disposal.

Methods of Disposal

Once equipment has been designated and approved for disposal, it shall be handled according to one of the following methods. It is the responsibility of the technology department to update the inventory system to reflect the disposal of the asset.

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.
Systems shall be wiped clean of this information prior to leaving the school district.

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.

**Donation**

In the event that the district determines that an asset shall be donated, an MOU must be approved by the Board. Since systems may contain Personally Identifiable Information (PII), Confidential, or Internal Information. Systems shall be wiped clean of this information prior to leaving the school district. In addition, Microsoft licenses or any other software licenses are not transferred outside the district. Therefore, systems must be returned to factory installation prior to donation.
Appendix I
Virus, Malware, Spyware, Phishing and SPAM Protection

Virus, Malware, and Spyware Protection
RQS 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. Raytown 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
Server patch management is performed weekly. Security patches are applied on an as needed basis, but at least weekly.
Appendix J
Account Management

Access controls are essential for data security and integrity. Raytown Quality 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 Raytown Quality 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 L: Data Access Roles and Permissions).
- Any exception to permissions must be approved by the district administrator responsible for the system (data manager) and the Chief Information Officer. This request must use the Additional Access Request form.

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.
- In all instances, the system account and associated network storage of the user that has separated from the District are immediately deleted on the termination date.

Local/DOMAIN Administrator Access

No user will be granted local administrator permissions unless required for the use of a specific software/application. If at all possible, technology staff will create custom scripts for these programs to run without the users having elevated permissions. In the event that a script cannot eliminate the need for elevated permissions, users may be made local machine administrators. All accounts needing this elevated permission
must be approved by the ISO. Once the elevated permissions are no longer required for the resource, the technology team will complete an audit of all user accounts and reinstate regular permissions.

Additionally, no users will have domain administrative access. Technicians requiring domain or local machine admin access will have a separate account for the sole purpose of this access. Technicians will use their regular district login (without elevated privileges) for all access not requiring elevated permissions.

**Remote Access**

Access into the District’s network from outside is strictly prohibited without explicit authorization from the ISO. Remote access will be granted through virtual private network (VPN) connection through the district’s network VPN appliance; no other method of remote access shall be granted 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 VPN access is needed by a contractor/vendor, access must be approved by the ISO. 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.

All VPN accounts will be reviewed at least annually.

**Contractors/Vendors**

Access to contractors/vendors is governed through the same process using Board of Education policy EHB-AP1 and EHB-AF4 (External User Technology Agreement). All contractor/vendor access must be approved by HR and ISO. 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 K
Data Access Roles and Permissions

Student Information System (SIS)

All staff members are entered into the SIS for the purpose of district badge printing. 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
- Work status
- Active
- Transfer
- 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
- Staff tracked but do not need access > Support No Access
- 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 including type of attendance and in/out time to the minute
  - View: Site Administrators, Counselors, Teachers
  - Maintain: Site Secretary
- Grades/Assessments including everything in the gradebook Assignments, Tests, Finals, etc.
  - View: Counselors, Site Administrators
  - Maintain: Site Secretaries, Teachers
- Programs and Services tracks many items including, Discipline, Waivers, 504s, SpEd (notes for Sped track), ELL, ESL, Medical, etc.
  - View: Anyone with access to search for student can see the icons at the top
  - Maintain: Specific to department
    - SpEd > SpEd track import
• Discipline > Building administrators
• Medical > Nurses

- Discipline
  o View: Counselors
  o Maintain: Site Administrators, Secretaries,
- Parent Communication (Email, Phone numbers, addresses)
  o View: Teachers, Site Administrators, Counselors, Librarian
  o Maintain: Residency
- Family Demographics
  o View: Secretaries, Site Administrators, Teachers, Nurses,
  o Maintain: Residency, District Administrators
- Fees
  o View: Site Administrators, Counselors
  o 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 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**

- Advanced Tech Users
- Basic View Only
- District Admin Support
- District Administrator
- District Core Data Coordinator
- District Curriculum Coordinator
- District Enrollment
- District Food Service Director
- District Registrar
- District Secretary
- District SpEd Director
- District SpEd View
- District Transportation
- Human Resources
- Site Administrator
- Site Counselor
- Site Day Care Office
- Site Food Service Manager
- Site Food Service POS Cashier
- Site Interventionist
- Site ISS Supervisor
- Site Librarian
- Site Nurse
- Site Secretary
- Site Social Worker
- Site SpEd Case Manager/Service Provider
- Site SpEd Coordinator
- Site Sub Teacher (Attendance Only)
- SpEd Assessment
- SpEd Teacher
- Sub Secretary
- Summer School Site Administrator
- Support - No Access
- Teacher
- Teacher Admin
- Technology
**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:

- Auditor
- Core Migration Team
- Director-SPED Principal
- Elementary
- Finance
- Human Resources
- Payroll
- Secondary
- SLT
- Technology Support

* A complete list of permissions is kept on file in the technology department.

**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 administrators in the Special Education department.

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

Special Education Administrators and district coordinators have access to all students in the district and assign building level access to building coordinators. Building coordinators assign student access to teachers and staff such as pathologists as needed.
Appendix L
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.
- Passwords shall be secure according to NIST recommended standards.
- When possible, user created passwords should adhere to the same criteria as required for district network access as outlined below.
- Passwords shall only be saved by district supported password lockers and single sign-on (SSO) systems as approved by the Technology Department.
- Passwords shall not be programmed into a PC or recorded anywhere that someone may find and use them.
- When creating a password for secure information or sites, it is important not to use passwords that are easily guessed due to their association with the user (i.e. children’s names, pets’ names, or birthdays).
- Users and employees who have reason to believe a password is lost or compromised must notify the ISO or designee as soon as possible. The technology department will verify the identity of the person requesting the change before resetting the password.

District network access to resources managed through Active Directory/SSO:

- Passwords must be “strong,” and must be a minimum of 16 characters long. The district encourages the use of passphrases, instead of passwords.
- Passphrases will only be changed in the event the user shares their passphrase with another employee or they believe their account has been hacked.
- You will not be allowed to use your three previous passwords.
- Your password must not be too similar to your username.
- Do not use your district passphrase for any non-district systems.

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

- Passwords routed over a network shall be encrypted.
- Passwords shall be entered in a non-display field.
- System software shall enforce the changing of passwords and the minimum length.
- 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 30 minutes.
- System software should maintain a history of previous passwords and prevent their being easily guessed due to their association with the user.
Appendix M
Technology Disaster Recovery Plan

Objectives

The primary purpose of the Technology Disaster Recovery Plan (TDRP) is to enable Raytown Quality Schools (RQS) 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 RQS TDRP:

- 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.
- District data is housed at district data center and backed up in the cloud.
- 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

RQS has appointed the following people to the disaster recovery/critical failure team: Chief Information Officer, Assistant Director of Technology Operations, Assistant Director of Technology Information Systems, Network System Administrator, Server System Administrator, and Database System Administrator.

In the event the TDRP 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 TDRP 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 TDRP implementation debrief.
**Activation**

The TDRP 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 Information Security Officer (ISO) will act as the incident response manager (IRM). If the ISO is not able to act as the IRM, a member of the Superintendent’s Leadership Team will assume the role of IRM, with assistance from the IRT.

**Notification**

The following groups will be notified 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 TDRP team will work with district leadership, including the Chief Communications Officer, on which information will be conveyed to each above group and what means will be used.

**Implementation**

The TDRP 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 hard copy of this document will be secured at the technology office and the Associate Superintendent of Operations’ office. An electronic version will be housed on Google Drive.
- Maintained spreadsheet of all local administrator accounts, passwords and vendor contact information. A hard copy of this document will be secured at the technology office and the Associate Superintendent of Operations’ office. An electronic version will be housed on Google Drive.
- The District’s data backup solution includes the use of a backup manager and off-site file storage, which backs up data locally in the datacenter and the cloud. The District’s critical virtual servers can be run
directly from the cloud with limited access.

- In the event of a critical system failure, the District can restore that server back to our current environment from the backup solution.

**Deactivation**

The TDRP team will deactivate the plan once services are fully restored.

**Evaluation**

An internal evaluation of RQS TDRP 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 TDRP and other emergency response plans as appropriate.
Appendix N
Data Breach Response Plan

Objectives

The purpose of the Technology Data Breach Plan (TDBP) is to enable Raytown Quality Schools (RQS) 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 TDBP are:

- Convene the Incident Response Team (IRT) 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, legal counsel, state/federal agencies and law enforcement as deemed necessary.

Planning Assumptions

The following planning assumptions were used in the development of RQS TDBP:

- 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 in the cloud.
- District data is hosted by 3rd party providers.

Data Breach/Incident Response Team

RQS has appointed the following people to the data breach/incident response team: Chief Information Officer, Assistant Director of Technology Operations, Assistant Director of Technology Information Systems, Network System Administrator, Server System Administrator, and Database System Administrator.

In the event the TDBP 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 Associate Superintendent of Operations.
- Coordinate with Chief Communications Officer to ensure communication with district staff and or parents as deemed appropriate.
- Oversight of the TDBP implementation and data breach resolution.
- Allocate and manage technology staff resources during the event.
- Work with vendors, 3rd party providers, manufacturers, legal counsel, state/federal agencies and law
enforcement while correcting the data breach and its repercussions.

- Oversight of TDBP implementation debrief.

**Activation**

The TDBP 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 (ISO) will act as the incident response manager (IRM). If the ISO is not able to act as the IRM, a member of the Superintendent’s Leadership Team will assume the role of IRM, with assistance from the IRT. The breach response and reporting process will be documented according to Policy EHBC-AP1, state and federal requirements. The Chief Information Officer will work with the Chief Communications Officer and Community Relations to dispense and coordinate the notification and public message of the breach.

**Notification**

The following groups will be notified 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 deemed appropriate. This could include any one or combination of the following:

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

The TDBP 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 TDBP team has the following processes in place to contain the data breach in the least of amount of time possible:

- Data inventory of all systems containing sensitive data. A hard copy of this document will be secured at the technology office and the Associate Superintendent of Operations’ office. An electronic version will be housed on Google Drive.
- Data dictionary of all district hosted information systems. A hard copy of this document will be secured at the technology office and the Associate Superintendent of Operations’ office. Due to non-disclosure agreements, this data may not be available in other locations/formats. The appropriate vendor(s) can be contacted for this information.
- Maintained spreadsheet listing all server names (servers.xlsx), physical and virtual, and their function. A hard copy of this document will be secured at the technology office and the Associate Superintendent of Operations’ office. An electronic version will be housed on Google Drive.
- Maintained spreadsheet of all system administrator accounts, passwords and vendor contact information. A hard copy of this document will be secured at the technology office and the Associate Superintendent of Operations’ office. An electronic version will be housed on Google Drive.
- The District’s data backup solution includes the use of a backup manager and off-site file storage, which backs up data locally in the datacenter and the cloud. The District’s critical virtual servers can be run directly from the cloud with limited access.

The following will take place during the incident response:

- The members of the IRT will be assembled once a breach has been validated. The IRT will be comprised of the Chief Information Officer, Assistant Director of Technology Operations, Assistant Director of Information Systems, Network Systems Admin, Database Systems Admin, and Server Systems Admin. Additional members of the Raytown School District administrative team and technology department may be designated to assist on the IRT.
- The IRT will determine the status of the breach, on-going, active, or post-breach. For an active and on-going breach, the IRT 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 IRT 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 IRM will work with legal counsel and the Superintendent’s Leadership Team 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 IRT will take place with the IRM. 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 IRT will work with the RQS 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 IRM to determine whether or not the Family Policy Compliance Office (FPCO) or PTAC needs to be notified.

• The IRM, in conjunction with the IRT, legal counsel and the Superintendent’s Leadership Team will determine if 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, and per Policy EHBC-AP1. If it is determined that identity theft or other fraud is not reasonably likely to occur as a result of the breach, such a determination shall be documented in writing and will be maintained for five years.

Deactivation

The TDBP team will deactivate the plan once the data breach has been fully contained.

Evaluation

Once the breach has been mitigated an internal evaluation of RQS TDBP response will be conducted. The IRT, in conjunction with the IRM 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 TDBP 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. Board Policy EHBC-AP1 may be modified at this time.