This page is intentionally left blank.
# Table of Contents

Purpose and Scope ........................................................................................................... 5

General Security Standards .............................................................................................. 5

Data Governance ................................................................................................................ 6

  Regulatory Compliance ............................................................................................... 7

Security and Data Governance Domains ......................................................................... 7

Security and Risk Management ....................................................................................... 8

Data Classification .......................................................................................................... 8

Data Classification Levels ............................................................................................. 8

  Personally Identifiable Information (PII) ................................................................ 8

  Confidential Information ............................................................................................ 8

  Internal Information .................................................................................................. 9

  Public Information ..................................................................................................... 9

  Directory Information ............................................................................................... 9

Risk Management ............................................................................................................ 10

Technology Staff: Roles and Responsibilities ................................................................. 11

Compliance ..................................................................................................................... 12

Maintenance of Policies, Standards, Guidelines and Recommendations ..................... 13

Related Policy and Procedure Documents ..................................................................... 13

  Board Policy and Technology Usage Agreement ..................................................... 13

  Incident Response Plan ............................................................................................. 13

  Technology Disaster Recovery Plan ......................................................................... 13

  Third Party Vendor Contracting Guide ...................................................................... 14

  Electronic Physical Access Control Guide ............................................................... 14

Asset Security .................................................................................................................. 14

  Software Standards and Procedures ......................................................................... 14

  Hardware Standards and Procedures ....................................................................... 15

  Mobile Devices .......................................................................................................... 16

  Practices for Network Use ......................................................................................... 16

Security Operations ......................................................................................................... 17

  Data Transfer/Exchange/Printing: ............................................................................ 17

  Electronic Mass Data Transfers ................................................................................ 17
Purpose and Scope

The purpose of this document is to outline procedures and standards regarding data governance, data security and individual privacy protection for the Park Hill School District. It is the duty of the Department of Technology to create an environment within the district that maintains system security, data integrity and privacy by preventing unauthorized access to data and by preventing misuse of, damage to or loss of data.

To create this document, the district has utilized Federal and State regulations as well as best practices and standards gathered from the U.S. Department of Education Privacy Technical Assistance Center (PTAC), the Information System Security Certification Consortium, the National Institute of Standards and Technology, the Consortium of School Networks (CoSN), and the Missouri Department of Elementary and Secondary Education.

For the purposes of this handbook, security is defined as the ability to protect the integrity, availability, and confidentiality of information held by the district, to protect its assets from unauthorized use or modification and from accidental or intentional damage or destruction. It includes the security of network facilities and off-site data storage; computing, telecommunications, applications and related services purchased from commercial concerns; and Internet-related applications and connectivity.

The Department of Technology will adhere to the standards identified in this document and use them to implement and maintain system and data security. Department staff will develop policies that govern the usage of district technology resources by all district staff and any other person who uses district technology.

General Security Standards

1. The district will operate in a manner consistent with the maintenance of a shared, trusted environment, for the protection of sensitive data and business transactions. The district will use consistent industry standard security protocols.

2. The district will establish its secure business applications within the guidelines of PTAC. This requires that all parties interact with agencies through a common security architecture and authentication process. The district will maintain and operate the shared infrastructure necessary to support applications and data within a trusted environment.

3. The district will operate its applications and networks within the appropriate guidelines and will subscribe to the following principles of shared security:
a. Follow security standards established for selecting appropriate assurance levels for specific application or data access and implement the protections and controls specified by the appropriate assurance levels.

b. Recognize and support a standard means of authenticating external parties needing access to sensitive information and applications.

c. Follow security standards established for securing servers and data associated with secure applications; and follow security standards established for creating secure sessions for application access.

4. The district will address use of the internet to conduct transactions for business with other public entities, citizens, and businesses in accordance with federal, state and local requirements.

5. The district will promote security awareness by informing employees, associates, business partners, or others using its computers or networks about security policies and practices, what is expected of them, and how they are to handle the information. All district employees will electronically sign the district Technology Usage Agreement, acknowledging their understanding of these polices, practices and expectations.

6. The district will ensure staff is appropriately trained in technology security procedures. The district will make staff aware of the need for technology security and train them to perform the security procedures for which they are responsible. This training will be conducted annually.

7. The district will review its technology security processes, procedures, and practices at least annually and make appropriate updates after any significant change to its business, computing or telecommunications environment.

8. The district technology security processes, procedures, and practices may contain information (confidential or private) about the district’s business, communications, and computing operations or employees. Therefore, any distribution of this or related documents will require consideration of sensitive information and related statutory exemptions for such information from public disclosure.

**Data Governance**

It is the policy of the district 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.

The district conducts annual trainings on data governance and documents those trainings. The terms data and information are used separately, together and interchangeably throughout this document. The intent is the same.
The Superintendent has authorized the Director of Technology to establish, implement, and maintain data and information security measures. These policies, 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.

All data governance rules, polices, regulations and guidelines apply to all forms of the district’s data and information, including but not limited to:

- Communication spoken in person, by phone or by 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, etc.
- Data stored and/or processed by servers, personal computers (PCs), laptops, tablets, mobile devices, etc.
- Data stored on any type of internal, external, or removable media or cloud-based services.

Regulatory Compliance

The district will abide by any law, statutory, regulatory, or contractual obligations affecting its data systems. The district complies with all applicable regulatory acts including but not limited to the following*:

- Park Hill School District Board policies and procedures
- Children’s Internet Protection Act (CIPA)
- Children’s Online Privacy Protection Act (COPPA)
- Family Educational Rights and Privacy Act (FERPA)
- Payment Card Industry Data Security Standard (PCI DSS)
- Protection of Pupil Rights Amendment (PPRA)

*See also Appendix A (Laws, Statutory, Regulatory and Contractual Security Requirements)

Security and Data Governance Domains

The district has separated all security and data governance elements into the following five distinct domains:

1. Security and Risk Management
2. Asset Security
3. Security Operations
4. Communication and Network Security
5. Identity and Access Management
Security and Risk Management

Data Classification

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 in compliance with Board Policy and any applicable laws. The classification assigned and the related controls applied are dependent on the sensitivity of the data. Data are 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.

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 for the district.

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:

- personnel information
- key financial information
- proprietary information of commercial research sponsors
- system access passwords
- information file encryption keys

Unauthorized disclosure of this information to people without a business need for access may violate laws and regulations, or may cause significant problems for the district, its staff including...
contract employees, parents, students or its business partners. Decisions about the provision of access to this information shall always be cleared through the information owner and/or a member of the Department of Technology Leadership Team. The members of this team include the Director of Technology, the Manager of Technology Support Services, the Manager of Network and Infrastructure, the Manager of Data Systems, and the Manager of Communications and Training.

Internal Information

Internal Information is intended for unrestricted use within the district, and in some cases, within affiliated organizations such as the district’s business or community partners. This type of information is already widely-distributed within the district, or it could be so distributed within the organization without advance permission from the information owner.

Examples of Internal Information may include:

- personnel directories
- internal policies and procedures
- most internal electronic mail messages

Any information not explicitly classified as PII, confidential or public shall, by default, be classified as Internal Information. Unauthorized disclosure of this information to outsiders may not be appropriate due to legal or contractual provisions.

Public Information

Public Information has been specifically approved for public release by a designated authority within the district. Examples of Public Information may include marketing brochures and material posted to the district’s website. This information may be disclosed outside of the district.

Directory Information

As defined in Board Policy JO, 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 of an eligible student. Directory information includes the following:

- Student name
- Parents’ names
- Grade level
- Enrollment status
- Identification number
- User id for electronic system access, if disclosure of that information alone cannot be used to access protected information
• Participation in district activities and/or sports
• Height and weight of members of athletic teams
• Dates of attendance
• Degrees and honors received
• Artwork or coursework displayed by the district
• Schools or districts previously attended
• Photographs, videos, recorded sound and digital images

Additionally, certain information may be disclosed to specific parties with legitimate education interests, as described in Board Policy JO. This limited directory information includes:

• Student address
• Student telephone number
• Student email address
• Parental addresses, telephone numbers and email addresses

Risk Management

A thorough risk analysis of all the district’s data networks, systems, policies, and procedures shall be conducted on an annual basis or as requested by the Superintendent or Director of Technology. The risk assessment shall be used as a basis for a plan to mitigate identified threats and risk to an acceptable level.

The Director of Technology administers periodic risk assessments to identify, quantify and prioritize risks. Based on the periodic assessment, measures are implemented that mitigate the threats by reducing the amount and scope of the vulnerabilities.

Because technology security planning is primarily a risk management issue, this handbook and its associated standards and guidelines focus on the creation of a shared and trusted environment, with particular attention to:

• Common approaches to end-user authentication
• Consistent and adequate network, server and data management
• Appropriate uses of secure network connections
• Closing unauthorized pathways into the network

The district’s use of the internet for conducting official business has generated the following security concerns:

• Information Integrity - Unauthorized deletion, modification or disclosure of information.
• Misuse - The use of information assets for other than authorized purposes by either internal or external users.
• Information Browsing - Unauthorized viewing of sensitive information by intruders or legitimate users.
• Penetration - Attacks by unauthorized persons or systems that may result in denial of service or significant increases in incident handling costs.
• Computer Viruses – Attacks using viral code that reproduces itself by modifying other programs, spreading across multiple programs, data files or devices on a system or through multiple systems in a network that may result in the destruction of data or the erosion of system performance.
• Fraud - Attempts to masquerade as a legitimate user to steal services or information, or to initiate transactions that result in financial loss or embarrassment to the organization.
• Component Failure - Failure due to design flaws or hardware/software faults can lead to denial of service or security compromises through the malfunction of a system component.
• Unauthorized additions and/or changes to infrastructure components.

To address these concerns, the district will take steps necessary to:

• Ensure secure interactions between and among business partners, external parties, and school districts to utilize a common authentication process, security architecture and point of entry.
• Prevent misuse of, damage to, or loss of district hardware and software facilities.
• Prevent unauthorized use or reproduction of copyrighted material by public entities.
• Ensure secure interactions between the district and outside agencies and ensure that there is a shared and trusted environment.
• Operate in a manner consistent with the Data Security Handbook and Board policies and procedures.
• Develop, implement, maintain and test security processes, procedures, and practices to protect and safeguard voice, video, and data computing and telecommunications facilities (including telephones, hardware, software and personnel) against security breaches.
• Train staff to follow security procedures and standards.
• Apply appropriate security measures when utilizing transactional internet-based applications.
• Ensure and oversee compliance with this policy.

Technology Staff Roles and Responsibilities

The district’s Department of Technology staff are responsible for developing and maintaining the district’s cybersecurity policies. Technology staff will:

• Develop and maintain this handbook and all associated policies, procedures, handbooks and guidelines.
• Research the technology industry for security related issues and determine how it affects the district technology infrastructure as a whole.
• Participate in local and/or national security organizations for the purpose of sharing security information, pitfalls, warnings, etc.

The Director of Technology and the Security Administrator will serve as contacts concerning all security-related issues. These individuals will:

• Develop and maintain district-specific security policies.
• Ensure that the district is adhering to State of Missouri and Department of Elementary and Secondary Education security policies.
• Maintain awareness of technology and security industry standards and events, especially any changes or issues which may affect the district directly.
• Monitor security issues within the district’s technology resources.

Compliance

All documents produced by the Department of Technology will comply with applicable laws and board policies. The Department of Technology will ensure all users of district technology are informed of the applicable laws, policies, procedures and guidelines for technology usage through periodic trainings and published documents.

Failure to comply with these policies by employees, staff, volunteers, and outside affiliates may result in disciplinary action up to and including dismissal in accordance with applicable district procedures, or, in the case of outside affiliates, termination of the affiliation. Failure to comply with this policy by students may constitute grounds for corrective action in accordance with the district’s policies. Further penalties associated with state and federal laws may apply.

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

• Unauthorized disclosure of PII or Confidential Information.
• Unauthorized disclosure of login information (User ID and password).
• An attempt to obtain login information that belongs to another person.
• An attempt to use another person’s login information.
• 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.
• Installation or use of unlicensed software on district technological systems.
• The intentional unauthorized altering, destruction or disposal of district information, data and/or systems. This includes the unauthorized removal from district technological systems such as but not limited to laptops, internal or external storage, computers, servers, backups or other media, copiers, etc. that contain PII or confidential information.
• An attempt to gain access to login information for purposes other than for support by authorized technology staff, including the completion of fraudulent documentation to gain access.

**Maintenance of Policies, Standards, Guidelines and Recommendations**

Technological advances and changes in the business requirements of the district will necessitate periodic revisions to policies, regulations, procedures, guides and handbooks. The district is responsible for routine maintenance of these to keep them current. Therefore, the Department of Technology Leadership Team will review and update technology security policies, regulations, procedures, guides, and handbooks at least annually or following any significant change to its business, computing or telecommunications environment. Examples of these changes include modifications to physical facilities, computer hardware or software, telecommunications hardware or software, telecommunications networks, application systems, organization or budget.

Practices will include appropriate mechanisms for receiving, documenting, and responding to security issues identified by third parties. Major policy changes require the approval of the Park Hill School District Board of Education.

If the district purchases technology services from another organization, the district and the service provider will work together to make certain the technology security plan for the service provider fits within the district’s security policies. The district will obtain a copy of the service provider’s data privacy and security plan to determine if it complies with district requirements.

**Related Policy and Procedure Documents**

**Board Policy and Technology Usage Agreement**

This document and its related procedures are governed by Board Policy EHB, EHB-C, and their associate regulations and forms. Response plans and process level procedures will adhere to the standards set by board policy. Anyone who uses district technology is required to sign and abide by the appropriate approved technology usage agreement.

**Incident Response Plan**

Technology staff will maintain an incident response plan detailing the district’s response and recovery to security events including physical intrusion of secured areas, electronic intrusions, deception and fraud, hacking incidents, or any other unplanned or unwanted security event posing a threat to district data and/or systems. (See Incident Response Plan)

**Technology Disaster Recovery Plan**
Technology staff will maintain a technology disaster recovery plan delineating the district’s procedures for recovery from an unforeseen disaster or emergency. This plan will contain process level procedures for recovering critical technology platforms, telecommunications infrastructure and ensuring data security. Controls shall ensure that the district can recover from any damage to critical systems, data, or information within a reasonable period of time. Each school, department, or individual will be required to report any instances immediately to the Department of Technology for response to a system emergency or other occurrence (e.g., fire, vandalism, system failure and natural disaster) that damages data or systems. The Disaster Recovery Plan shall include the following:

- A prioritized list of critical services, data and contacts.
- A process enabling the district to restore any loss of data in the event of fire, vandalism, natural disaster or system failure.
- A process enabling the district to continue to operate in the event of fire, vandalism, natural disaster or system failure.
- Procedures for periodic testing of written contingency plans to discover weaknesses and the subsequent process of revising the documentation, if necessary. (See Disaster Recovery Plan)

Third Party Vendor Contracting Guide

Technology staff will adhere to the guidelines defined in the Third Party Vendor Contracting Guide, which ensures the security of student and district data when dealing with external companies or agencies. (See Contracts with Third Party Vendors)

Electronic Physical Access Control Guide

The Department of Technology maintains an access control guide. This guide outlines how ID cards are issued and recovered as well as how access is granted.

Asset Security

Software Standards and Procedures

The district shall abide by the following standards and procedures regarding all software that it owns or licenses:

- Software owned or licensed by the district may not be copied to alternate media (such as removable hard drives), distributed by email, transmitted electronically, or used in its original form on any device other than district resources without express permission from the Department of Technology.
• Software licensed to the district is to be used for its intended purpose according to the license agreement. Employees are responsible for using software in a manner consistent with the licensing agreements of the manufacturer. In no case is the license agreement or copyright to be violated. License agreements are maintained by the Department of Technology.
• All software installed on district computers must be owned or licensed by the district. (See also Contracts with Third Party Vendors)
• All software purchased by the district must be installed on district-owned equipment, and may not be taken off-site without permission from the Department of Technology.
• No district owned software may be installed on a computer not owned by the district unless the license agreement specifically allows it and the installation is overseen by technology staff.
• There must be a separate software license for each computer unless a site license is purchased. Users may not purchase one software program or compact disc and install it on additional computers, such as every computer in the room.

Hardware Standards and Procedures

The district shall abide by the following standards and procedures regarding all hardware that it owns or leases:

• All workstations, printers, add-in cards, memory modules, and other associated equipment are the property of the district and should not be used for purposes other than those relevant to the execution of duties or sanctioned educational activities.
• No changes, modifications, additions, or equipment removals may be done without written notification to and approval from the Department of Technology.
• No information systems equipment should be removed from the district, with the exception of documented approval, from the Director of Technology or his/her designee, for equipment to be used for off-site by a named, specific staff member.
• Unless otherwise authorized by a member of the Department of Technology Leadership Team, all computer and network electronics connected to the district network must be owned/leased by the district and must be on the fixed asset inventory.
• The fixed asset inventory of all end-user devices will be maintained by the Manager of Technology Support Services and will include the Device Name, Serial Number, Asset Tag Number, Location and Purpose that each device is being used for.
• The fixed asset inventory will be maintained in a database and updated as needed.
• A full walk-through inventory inspection will be conducted by the Department of Technology at least two times per year, under the supervision of the Manager of Technology Support Services.
• A standard platform is established for district computers and equipment by the Department of Technology Leadership Team and documented by the Manager of Technology Support Services.
• Non-standard hardware is only to be used if standard hardware is unavailable and only if approved by the Department of Technology Leadership Team.
• All hardware purchased by the district must be installed on district-owned equipment.
• In order for effective software and network functioning, the district will make every effort to provide up-to-date and reliable hardware, including computers, servers, routers, switches, etc.

Mobile Devices

A mobile device is defined as any handheld network capable computing device such as a smartphone or tablet. The district has established procedures which allow it to keep track of mobile devices used to access district information and the personnel who use them.

The Department of Technology will adhere to the following concerning mobile devices given to district personnel:

• If the device supports a passcode feature, the passcode lock shall be enabled at all times and entered by the user for access. The passcode lock shall be active when the device is idle.
• The loss or theft of a device must be reported to both the Department of Technology Help Desk and the user’s immediate supervisor as soon as the loss or theft is identified.
• Devices which have been configured to access district information or electronic mail shall have the capability to be remotely erased and rendered unusable.
• The Department of Technology will maintain record of all assigned devices using the Mobile Device Inventory.

Practices for Network Use

In accordance with Board Policy EHB-R, authorized employees may use the district’s technology resources for reasonable, incidental personal purposes as long as the use does not violate any provision of district policies or procedures, hinder the use of the district’s technology resources for the benefit of its students or waste district resources. The following requirements must be followed by all network users:

• No materials, physical or digital, are to be disseminated in any manner which are derogatory to any person or group, obscene, racist, sexist, harassing or offensive based on color, religion, creed, national origin, age or disability.
• System identification codes and passwords are for the use of the specifically assigned user and are to be protected from abuse and/or use by unauthorized individuals.
• All email messages are automatically scanned for viruses using the virus detection software installed on all computer workstations. If a user makes any configuration changes to their workstation, even with the approval of the Department of Technology, it is their responsibility to ensure virus protection before opening/executing external media, email attachments, executable email messages, or downloaded files or programs.
• All district technology resources including internet access and email are for work and education purposes only. Access and sites visited can and will be monitored at the specific individual level.
• Employees may not use district technology resources for soliciting, personal financial gain, partisan political activities or further disseminating junk email such as chain letters.
• Information contained on the district’s network and workstations is strictly proprietary to the district. All data stored on district computers and/or servers are the property of the district. Copying or disseminating any of this information for any purpose other than district business is strictly prohibited. Access to this information must be considered confidential.

• Users are expected to report any observed violations of district technology policies and procedures to the Department of Technology and their immediate supervisor or, in the event that the violation involves the supervisor, the next appropriate level of authority. All incidents and actions should be documented by the Security Administrator and kept by Human Resources/Student Services. The Security Administrator will keep a record of technical action taken, while Human Resources and Student Services will keep a record of the incident and related consequences.

• Any user who knowingly and willingly violates district technology policy is subject to discipline up to and including termination from employment, or expulsion from school, depending on the severity of the specific offense(s). Furthermore, in the event of an illegal activity, the user will also be reported to the appropriate law enforcement authority.

Security Operations

Data Transfer/Exchange/Printing:

Electronic 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 this handbook and all related board policies and procedures, and must be approved by the Department of Technology Leadership Team. All mass downloads of information shall include only the minimum amount of information necessary to fulfill the request and will adhere to the security policies and procedures described in the Third Party Vendor Contracting Guide.

Other Electronic Data Transfers and Printing

PII, Confidential Information, and Internal Information shall be stored in a manner inaccessible to unauthorized individuals. PII and Confidential Information shall not be downloaded, copied or printed indiscriminately or left unattended and open to compromise. PII that is downloaded for educational purposes where possible shall be de-identified before use.

Oral Communications
The district’s 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. District 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 on public transportation.

Audit Controls

Hardware, software, services and/or procedural mechanisms that record and examine activity in information systems that contain or use PII are reviewed by the Department of Technology staff annually. Department of Technology staff also regularly review records of information system activity, such as audit logs, access reports and security incident tracking reports.

Evaluation

The district requires that periodic technical and non-technical evaluations of access controls, storage, and other systems be performed in response to environmental or operational changes affecting the security of electronic PII to ensure its continued protection.

Security Incident Reporting

A security incident is defined as any event posing a threat to district data or systems. All security violations or suspected violations must be reported to the Department of Technology. The Department of Technology may take any measures deemed appropriate for the specific security violation as outlined in the Incident Response Plan.

The Department will also work with the appropriate administrative party to ensure evidence is preserved and reported correctly, and contact appropriate law enforcement if deemed necessary by the Incident Response Team.

It is the responsibility of all district staff and any persons who utilize district technology to report suspected security violations as quickly as possible. Security breaches may be categorized as those pertaining to physical intrusions; electronic intrusions that include networks, servers and workstations; incidents related to catastrophic disasters; and breaches as a result of deception and/or fraud. Regardless of the category of incident, the district’s focus is the protection of district assets, containment of damage and the restoration of service.

Security and Data Logs

The Department of Technology archives specific log file types for a pre-defined duration. Documentation around specifically which logs are kept and what information they contain is documented in this handbook under Network Security Administration Procedures.
Communication & Network Security

Firewall Requirements: Use, Functionality and Port Restriction

The district will maintain firewalls that provide borders of protection between the internal network and the connection to the internet. Below are examples of what will not be permitted:

- No File Transfer Protocol (FTP) access is allowed from the internet to a device on the district network.
- The district will not restrict FTP out of the network to a device on the internet provided that session/transfer is initiated from the network.
- No Local Area Network (LAN) protocols will be mapped to and/or from devices on the internet (e.g., NetBios, NetBeui, NFS).
- No outbound port that has the potential of propagating industry known viruses, worms, etc. will be allowed.
- For email restrictions see Email Functionality, Security and Limitations (Page 16)

The exception to these port restrictions is when the district has a VPN implemented between them and a third party. In that scenario, all ports are available for use provided the traffic goes through the VPN.

At no time will the district permit a third party entity to connect directly to their local area network behind the firewall. This includes terminating third party circuits behind firewalls and/or utilizing a PC remote control product (e.g., PC Anywhere).

Web Server: Connectivity and Security

The district maintains and houses web servers that reside on the district network and are accessible from the internet. The district is required to “harden” the server by making sure that all the current operating system patches are applied and kept up to date and by removing any unnecessary server processes. Web servers shall not be accessible directly from the internet and should only be accessible through a firewall and/or load balancer.

Email Functionality, Security and Limitations

For the purpose of security and limiting spam into the network, the district shall require vendors of services to implement and maintain mail relays on the inside of the firewall. All mail must come through the mail relay and be “relayed” to the appropriate mail server.

- No direct Simple Mail Transfer Protocol (SMTP) from the internet. The district will utilize the mail relays for mail traveling in from the internet.
- No Post Office Protocol (POP) or Internet Message Access Protocol (IMAP) from internet to mail servers inside the network. The district will utilize a web interface Hypertext Transfer Protocol/Hypertext Transfer Protocol Secure (HTTP/HTTPS) to access this mail.
• No POP or IMAP from the network to private mail accounts on internet. The district will utilize a web interface (HTTP/HTTPS port) to access this mail.
• Users will be instructed to never open any email attachments on the network except via district email. Users will be instructed to use extreme caution when opening email attachments to ensure that the attachment is safe. Virus scanning is used on the district email system.

Non-Educational/District-Business Related Network Traffic

Bandwidth has a high cost associated with its usage. The district network is implemented and maintained to allow district employees to utilize automated systems and tools to facilitate their responsibilities and duties and meet the needs of those individuals they serve. The district network infrastructure must not be utilized for personal gain and/or entertainment.

Unnecessary applications that pose potential security risks will not be permitted. Peer to peer file sharing services and any other illegal software or services will not be permitted on district networks. There are legal ramifications tied to users who use these applications to share files. Users may only use properly licensed software and audio or video media purchased by the district or approved for use by the district. All users will adhere to the limitations of the district’s technology licenses. Copying for home use is prohibited unless permitted by the district’s license and approved by the district.

Wireless Access Connectivity

The district will enable and configure encryption on all wireless traffic.

No installations of wireless devices, such as wireless access points, wireless printers, or wireless network cards may be installed in the district by any person except technology staff. Proper configurations must be performed in order to protect the network.

Consideration for wireless connections will be based upon the need for the connection, as well as assuring security and integrity of the network. Wireless access may be denied at the discretion of a member of the Department of Technology Leadership Team.

Internet Filtering

The district will use the Barracuda filtering server(s) located at the core to provide content filtering. The district will utilize proxy servers for the purpose of tracking internet usage. The district will be CIPA compliant.

If parents/guardians request stronger internet filtering for their student, he/she will be added to the designated strict internet filter group.

Virus Prevention, Detection and Removal

The district will:
• Maintain real-time anti-virus software on the network including all servers and workstations
• Be diligent about keeping virus definition files up-to-date
• If a device is infected with a virus, the offending machine will be removed from the network until such time the virus can be removed from the machine.
• Ensure copies of virus-detection and eradication tools are kept offline to prevent any virus from modifying the detection tools. Technology staff will actively scan/check for viruses online, but periodically use the offline, trusted copies of the tools to scan the systems.
• Virus checking systems approved by the Department of Technology are deployed using a multilayered approach (computers, servers, gateways, firewalls, filters, etc.) that ensures all electronic files are appropriately scanned for viruses, malware, spyware, phishing and spam. Users should not turn off or disable the district’s protection systems or install other systems.

**Network Security Administration Procedures**

• Normal logging processes must be enabled on all host and server systems. Detailed information about logging requirements and retention is documented in the Event Logging Guide.
• Alarm and alert functions, as well as logging of any firewalls and other network perimeter access control systems must be enabled.
• Audit logs from the perimeter access control systems should be reviewed on a regular basis.
• Audit logs for servers and hosts on the internal, protected network should be reviewed on a regular basis
• Users must be trained to report any abnormalities in system performance to technology staff.
• Users must notify the Department of Technology of violations of the CIPA law. All users must abide by CIPA. Violations will be reported to the proper legal authorities.
• All incident reports received by the Department of Technology must be reviewed for symptoms that might indicate intrusive activity. Suspicious symptoms must be reported to the appropriate Manager within the Department of Technology and the Technology Security Administrator
• Any user who witnesses or suspects a security incident of any kind must report it to the Department of Technology immediately. All security incidents will be dealt with following the procedures described in the Technology Incident Response Plan.

**Identity and Access Management**

**Access Controls**

Physical and electronic access to information systems that contain Personally Identifiable Information (PII), Confidential Information, Internal Information and computing resources is controlled. To ensure appropriate levels of access by internal workers, a variety of security measures are instituted as approved by the Department of Technology Leadership Team. In particular, the Technology Leadership Team will document roles and rights to the student information system and other like systems.
Mechanisms to control access to PII, Confidential Information, Internal Information and computing resources include, but are not limited to, the following methods:

Authorization

Access shall be granted on a “need to know” basis and shall be authorized by the Superintendent, principal, immediate supervisor, or Department of Technology Leadership Team. Specifically, on a case-by-case basis, permissions may be added in to those already held by individual users in the student management system, again on a need-to-know basis and only in order to fulfill specific job responsibilities, with approval of the Department of Technology Leadership Team.

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 shall be held accountable for all actions performed on the system with their user ID. User accounts and passwords will not be shared.

Logon Banner

The Department of Technology will ensure that a logon banner will be displayed to users when they log on to district devices. The logon banner should include information regarding the district’s policies on privacy and security and should be in compliance with applicable laws and regulations.

Data Integrity

The district provides safeguards so that PII, Confidential, and Internal Information is not altered or destroyed in an unauthorized manner. Core data are backed up to a private cloud for disaster recovery. In addition, listed below are methods that are used for data integrity in various circumstances:

- Transaction audit
- Disk redundancy (RAID)
- ECC (Error Correcting Memory)
- Checksums (file integrity)
- Data encryption
- Data wipes

Transmission Security

Technical security mechanisms are in place to guard against unauthorized access to data that are transmitted over a communications network, including wireless networks. Integrity controls and encryption (such as SSL) are implemented where deemed appropriate.
Remote Access

Access into the District’s network from outside is allowed using the Park Hill Application Portal. All other network access options are strictly prohibited without explicit authorization from the Department of Technology Leadership Team. Furthermore, PII, Confidential Information and/or Internal Information that is stored or accessed remotely should maintain the same level of protections as information stored and accessed within the district’s network. PII should only be stored in cloud storage if said storage has been approved by the Department of Technology Leadership Team.

User Accounts

District user accounts are automatically assigned according to the user’s job code in the Human Resources System. This includes levels of permissions for each account. The Department of Technology Leadership Team will review the HR job codes once per year to ensure that the correct level of permission and access is assigned.

Requests for Additional Access and/or Permissions

Users requesting additional access or permission levels will submit a Help Desk request. The ticket will be escalated to the Manager of Technology Support Services who will then work with the appropriate technology manager to consider whether the request should be granted, and if so, determine:

- The needed duration of the escalated access or permission.
- If the needed access or permission is a requirement for a particular individual or if it should be assigned to the HR job code.

Passwords

Passwords are personal identification keys that allow access to various technology resources on the district’s network. Passwords help ensure that only authorized individuals gain access to a computer system, network device, application, file, data, etc. Passwords also help to establish accountability for all transactions and changes made to those technology resources. The district has enacted strict password policies in securing our local network. The following guidelines are used when developing password policies, with the exception of students in kindergarten through second grade.

Password Creation Requirements

- Passwords must contain at least six nonblank characters.
- Passwords must be changed at a minimum of every 365 days and not more than every 30 days.
- New passwords must not be any of the previous two passwords.
- Passwords should contain a combination of letters and numbers.
• Passwords should not contain the user ID.
• Passwords should not include any personal information about the user that can be easily guessed: user’s name, spouse’s name, kid’s name, employee number, Social Security number, initials, pet’s name, birthdate, telephone number, city, etc.
• Passwords should not consist of only common words from an English dictionary or foreign-language dictionary.
• Passwords should not contain commonly used proper names, including the name of any fictional character or place.
• Passwords should not contain any simple pattern of letters or numbers such as "qwertyxxx" or "xyz123xxx."
• Passwords should not be trivial, predictable or obvious.
• Passwords should be memorized and not displayed for others to view.

Default Passwords

• The default password for all new users, as well as all users needing to reset their passwords will be the user’s birthdate in the following format:

   (Month [3 Digits]).(Birth Year [4 Digits])

   For example: mar.1994

• Default passwords must be reset at first login and are bound by all other password requirements.
• Parents requesting to change a student’s password must verify their student's date of birth.
• Students will be bound by the same password requirements as staff.
• Default passwords will not be recorded in an "initial password" field in the Student Information System.
• User passwords can only be reset to the default password by calling the Department of Technology Help Desk.
• The Help Desk will verify the user’s date of birth before resetting the password back to the default password. Help Desk personnel should not recite the user’s birth date out loud.

Protecting Passwords

• Passwords will be required on all user accounts.
• Passwords must be unique to the users.
• Passwords must not be disclosed to anyone except when there is an overriding operational necessity (e.g., support issue).
• Passwords must be changed if anyone other than the authorized user learns the password.
• Passwords must not be left in a location accessible to others or secured in a location for which protection is less than that required for information that the password protects.
• Users must avoid sending passwords in clear text over the network.
• Passwords must be changed at least every school year and never reused.
• If a support vendor requires temporary access to district technology resources, their access must be restricted to that which is necessary for their function, and must be immediately revoked upon completion of their support task.
• User accounts for staff no longer employed by the district will be removed automatically following the employee’s last access date in the Human Resources system.
• Users must lock or log off when leaving their computer.
• All student and staff computers will be automatically locked after 15 minutes of inactivity.
• Teachers and/or staff members must never allow another user (such as a student or substitute teacher) to use their computer while they are logged in to the network. Teachers and staff have more privileges than students, such as access to grade books, and students should never have access to those rights.
• Students may never use another student, teacher, or staff member’s password nor may they use a computer that is already logged in as another user.
• If a user suspects their password has been cracked or stolen, they must inform the Department of Technology and change their password immediately.

Physical Access: Security Guidelines and Recommendations

The district recognizes that a majority of security incidents, vandalism, and even accidental acts that lead to disruption of services can be attributed to deficiencies in physical security. The guidelines below were established in order to maintain adequate physical security for the district.

Responsibility

The Manager of Technology Support Services is responsible for the physical security of district end-user devices. This includes but is not limited to desktops, laptops, cell phones, hotspots, monitors, printers, projectors, televisions and SmartBoards.

The Manager of Network and Infrastructure is responsible for the physical security of district network devices. This includes but is not limited to switches, routers, servers, racks, access points and security cameras.

Location

• Network equipment will be located in inconspicuous places without maps and external references.
• Network and computer equipment will be located away from windows or any other place that allows easy access by outside individuals.
• Network equipment and computer equipment will be located in places that can be environmentally controlled.
Access

- Rooms or closets that contain District Wide Area Network routers and servers must be locked at all times, including remote offices. Department of Technology staff are the only authorized party to enter these rooms.
- Wiring closets must be locked at all times. Department of Technology staff are the only authorized party to enter these closets.
- Switches are to be secured in a lock protected closet. Department of Technology staff are the only authorized party to enter these closets.
- A secure access system should be installed and maintained in the main datacenter(s). Only authorized personnel are allowed access to the datacenter(s) without an escort.
- All users must log off the network when they walk away from the computer. No computer connected to the network should ever be left unattended by the user who logged in to the network. All users must log off the network and the computer at the end of the day.
- All classrooms, offices, meeting rooms, etc. that house computers must be locked and secured when the room is vacated.

PII, Confidential and Internal information Access

- Access to areas in which information processing is carried out shall be restricted to only appropriately authorized individuals. At a minimum, staff passwords shall be changed annually.
- No PII, Confidential and/or Internal Information shall be stored on a device itself such as a hard drive, mobile device of any kind, or external storage device that is not located within a secure area.
- No technological systems that may contain information as defined above shall be disposed of or moved without adhering to the appropriate Purchasing and Disposal of Electronic Equipment procedures.
- It is the responsibility of the user to not leave these devices logged in, unattended and open to unauthorized use.

Environmental and Electrical Measures

At a minimum, district datacenters and telecommunications rooms should employ the following environmental controls:

- Fire protection in these areas shall comply with NFPA 75: Standard for the Fire Protection of Information Technology Equipment and NFPA 76: Standard for the Fire Protection of Telecommunications Facilities.
- Electrical systems for critical computer equipment must include Uninterrupted Power Systems (UPS). Surge protectors should be considered for equipment sensitive to power fluctuations, at the discretion of the Manager of Network and Infrastructure.
- Adequate room temperature and humidity must be maintained to the specifications of the hardware vendor.
Appendix A
(Laws, Statutory, Regulatory and Contractual Security Requirements)

A. **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.

For more information, see: [http://www.fcc.gov/guides/childrens-internet-protection-act](http://www.fcc.gov/guides/childrens-internet-protection-act)

B. **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. See [www.coppa.org](http://www.coppa.org) for details.

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

D. **PPRA**: The Protection of Pupil Rights Amendment affords parents and minor students’ rights regarding our conduct of surveys, collection and use of information for marketing purposes, and certain physical exams. These include the following:

A right to consent before students are required to submit to a survey that concerns one or more of the following protected areas (“protected information survey”) if the survey is funded in whole or in part by a program of the U.S. Department of Education (ED)—

1. Political affiliations or beliefs of the student or student’s parent;
2. Mental or psychological problems of the student or student’s family;
3. Sex behavior or attitudes;
4. Illegal, anti-social, self-incriminating or demeaning behavior;
5. Critical appraisals of others with whom respondents have close family relationships;
6. Legally recognized privileged relationships, such as with lawyers, doctors or ministers;
7. Religious practices, affiliations, or beliefs of the student or parents; or
8. Income, other than as required by law to determine program eligibility.
A right to receive notice and an opportunity to opt a student out of –

1. Any other protected information survey, regardless of funding;

2. Any non-emergency, invasive physical exam or screening required as a condition of attendance, administered by the school or its agent, and not necessary to protect the immediate health and safety of a student, except for hearing, vision or scoliosis screenings, or any physical exam or screening permitted or required under state law; and

3. Activities involving collection, disclosure, or use of personal information obtained from students for marketing or to sell or otherwise distribute the information to others.

For more information, see: http://www2.ed.gov/policy/gen/guid/fpco/ppra/index.html