Cybersecurity Policy

PAMPA INDEPENDENT SCHOOL DISTRICT

BOARD APPROVED DECEMBER 19, 2019

Contents

Cybersecurity Policy
Pampa Independent School District

Section 1

Introduction

The possibility that electronic information could be lost, corrupted, diverted, or misused represents a real threat to business-critical functions and personal information of staff and students of Pampa ISD. Pampa ISD is more dependent than ever on information technology. Information technology has gone from being important to being critical in the daily functions of Pampa ISD. However, as Pampa ISD's dependence on information technology has grown, so too has the vulnerability of this technology and the range of external threats to this technology.

Cybersecurity is a key aspect of the interaction among many important societal issues – defense, terrorism, commerce, privacy, intellectual property rights, and computer crime. Information technology resources also consume a growing share of the Pampa ISD budget and are becoming increasingly important to daily life. As a result, a considerable body of applicable policy is in place, consisting of laws, statutes, regulations, and other directives. Pampa ISD Cybersecurity Program must operate within this complex policy landscape to ensure that Pampa ISD meets its obligations to its employees and students. Providing for the security of information resources is not only a difficult technical challenge, it is also a human challenge. Ultimately, cybersecurity is a human endeavor that depends heavily on the behavior of individual end users.

Purpose

By cybersecurity we mean the protection of Pampa ISD data, applications, networks, and computer systems from unauthorized access, alteration, or destruction.

The purpose of the Cybersecurity Policy is:

- To establish a district-wide approach to information security.
- To prescribe mechanisms that help identify and prevent the compromise of cybersecurity and the misuse Pampa ISD data, applications, networks and computer systems.
- To define mechanisms that protect the reputation of Pampa ISD and allow Pampa ISD to satisfy its legal and ethical responsibilities with regard to its networks' and computer systems' connectivity to world-wide networks.

- To prescribe an effective mechanism for responding to external complaints and queries about real or perceived non-compliance with this policy.

General Policy

Throughout the document the terms *must* and *should* are used carefully. The term *must* is non-negotiable; the term *should* is a goal for Pampa ISD.

- Pampa ISD will use a layered approach of overlapping controls, monitoring and authentication to ensure overall security of Pampa ISD employee and student data, networks, and system resources.
- Security reviews of servers, firewalls, routers and monitoring platforms should be conducted on a regular basis. These reviews must include monitoring access logs and results of intrusion detection software, where it has been installed.
- Vulnerability assessments of external and internal (authenticated) connections must be conducted on a regular basis. At a minimum, assessments should be performed quarterly, but the sensitivity of the information secured may require that these assessments be conducted more often.
- Education should be implemented to ensure that all users understand data sensitivity issues, levels of confidentiality, and the mechanisms to protect the data. This should be tailored to the role of the individual (e.g., network administrator, business manager, users).

Ownership

The Cybersecurity Policy is owned by Pampa ISD. Pampa ISD Technology Department, with the approval of the School Board, is the only authority that can approve modifications to the Cybersecurity Policy.

Disciplinary Action

Violation of Pampa ISD Cybersecurity Policy may result in disciplinary actions as authorized by the Superintendent in accordance with Pampa ISD disciplinary policies, procedures and codes of conduct. Additionally, individuals are subject to loss of Pampa ISD information resources access privileges, as well as civil and criminal prosecution. Violations of this policy or aggregate security policies/procedures are subject to the guides previously established in the Violations and Disciplinary Actions Policy of Pampa ISD.

Security Policy Development and Maintenance Procedures

Introduction

The Pampa ISD Cybersecurity Policy provides the operational detail required for the successful implementation of the Information Security program adopted by the district. These individual security policies/procedures have been developed by interpreting Family Educational Rights and Privacy Act (FERPA), Texas Administrative Code, Chapter 202 (TAC 202), Senate Bill 820, House Bill 3834, grant guidelines, other legislation and legal requirements, understanding business need, evaluating existing technical implementations and by considering the cultural environment.

Purpose

The legal, business, technical and cultural environment of Pampa ISD, as it relates to information resources use and security, is constantly changing. This Cybersecurity Policy is technology neutral and applies to all aspects of information resources. Emerging technologies or new legislation, however, will impact this Cybersecurity Policy over time. The Cybersecurity Policy will be revised, as needed, to comply with changes in federal, state, or local laws or rules promulgated there under or to enhance its effectiveness.

Scope

The Cybersecurity Policy applies to all Pampa ISD employees and all Pampa ISD owned information resources including, but not limited to, hardware, software, applications, cloud services, electronic and hardcopy data sources, file shares, and peripherals.

Procedures

A number of factors could result in the need or desire to change Pampa ISD Cybersecurity Policy. These factors include, but are not limited to:

- Review schedule
- New federal, state, local legislation
- New grant guidelines
- Newly discovered security vulnerability/vulnerabilities
- New technology
- Audit report
- Business requirements
- Cost/benefit analysis
- Cultural change

Updates to the Cybersecurity Policy, which include establishing new policies, modifying existing polices or removing policies can result from three different processes:

- At least annually, the Director of Information Technology, or designee, will review current policies for possible addition, revision, or possible deletion. An addition, revision or deletion is created if it is deemed appropriate.
- Every time new information resource technology is introduced into Pampa ISD, a security risk assessment should be completed. The result of the security risk assessment could necessitate changes to the Cybersecurity Policy prior to the new technology being approved for use.
- Updates to the Cybersecurity Policy will be made following any major changes to federal, state, or local legal statutes or grant guidelines within sixty (60) days of announcements.
- Any user may propose the establishment, revision or deletion of any practice standard at any time. These proposals should be directed to the Director of Information Technology who will evaluate the proposal and make recommendations to the Superintendent. Once a change to the Cybersecurity Policy has been approved by the School Board, the following steps will be taken as appropriate to properly document and communicate the change:
  - The appropriate information sources (e.g., Employee Handbook and Student Code of Conduct) will be updated with the change.
  - Changes will be communicated to all users through the Pampa ISD Technology Department.
  - Any necessary trainings will be offered.

Section 2

Password Policy

Overview

Passwords are the primary form of user authentication used to grant access to Pampa ISD information systems. To ensure that passwords provide as much security as possible, they must be carefully created and used. Without strict usage guidelines, the potential exists that passwords will be created that are easy to break, thus allowing easier illicit access to Pampa ISD information systems, and thereby compromising the security of those systems.

Purpose

The purpose of this Password Procedure is to establish the rules for the creation of strong passwords utilized to access Pampa ISD information systems.

Scope

The scope of this procedure includes all personnel who have or are responsible for a user account on any information system or service that Pampa ISD owns or manages.

Procedures

General

a. All usernames will consist of the user’s first and last names respectively, separated by a period.
b. All domain and email passwords must be changed annually, and the previous two password~~s~~ cannot be reused.
c. All domain and email passwords must conform to the guidelines described below:
   i. Be a minimum of fourteen (14) characters on all systems.
   ii. Must not be the same as or contain the username.
   iii. Must not be transmitted in clear or plain text outside of Pampa ISD.
   iv. Must not be written on paper or any medium that can be accessed by others.
   v. Must not be displayed when entered.

Password Protection Standards

a. Passwords must not be shared with ANYONE.
b. If someone demands a password, refer them to this document or have them call the Director of Information Technology or designee.
c. If an account or password is suspected to have been compromised, report the incident to your supervisor or the Director of Information Technology or designee, and change all passwords immediately.
d. All domain and email accounts will be locked after ten (10) failed password attempts.

Revision History

Date of Change	Author	Rationale
11/14/2019	Dennis Boyd & Melody Baker	Initial implementation

Network Access Procedures

Overview

The Pampa ISD infrastructure is provided as a central utility for all users of Pampa ISD information resources. It is important that the infrastructure, which includes cabling and the associated ‘active equipment’, continues to develop with sufficient flexibility to meet Pampa ISD demands while, at the same time, remaining capable of exploiting anticipated development in high speed networking technology to allow the future provision of enhanced user services.

Purpose

The purpose of the Network Access Procedures is to establish the rules for the access and use of the network infrastructure. These rules are necessary to preserve the integrity, availability, and confidentiality of Pampa ISD information.

Scope

The scope of these procedures applies to all Pampa ISD employees and students (users) with access to Pampa ISD infrastructure and information resources.

General Procedures

1. Users are permitted to use only those network addresses issued to them by the Technology Department.
2. All remote access to Pampa ISD will be through an approved VPN connection.
3. Remote users may connect to Pampa ISD resources only through methods and using protocols approved by Pampa ISD.
4. Users must not install network hardware or software that provides network services without written approval from the Director of Information Technology or designee. This includes, but is not limited to, wireless access points, modems, and remote access software.
5. Non-Pampa ISD computer systems that require network connectivity must be approved, in writing, by the Director of Information Technology or designee.

6. Users must not download, install, or run security programs or utilities that reveal weaknesses in the security of a system. For example, Pampa ISD users must not run password cracking programs, packet sniffers, network mapping tools, or port scanners while connected in any manner to the Pampa ISD network infrastructure unless stated in job responsibilities or with written approval from the Director of Information Technology or designee.
7. Users are not permitted to alter network hardware in any way unless stated in job responsibilities or with written approval from the Director of Information Technology or designee.

Network Usage Guidelines

1. Personal Safety
    a. Users understand the risk of posting personal contact information and Pampa ISD cannot be held responsible for the consequences of such actions. Users will not post personal information for or about others without their permission. Personal contact information includes, but is not limited to, address, photos and/or telephone numbers.
    b. Users will promptly disclose to supervisor or designee of any message received via email that is inappropriate or makes them feel uncomfortable.
2. Illegal Activities
    a. Users will not attempt to gain unauthorized access to the Pampa ISD network or resources beyond their assigned authorized access. This includes attempting to log on through another employee’s account or access another employee’s files without their knowledge or consent.
    b. Users will not make deliberate attempts to disrupt the Pampa ISD network and/or resources or destroy data by spreading computer viruses or by any other means.
    c. Users will not use access to the Pampa ISD network or resources to engage in any illegal act.
    d. Users will not read, move, rename, edit, or in any way alter the files that have been created or organized by others without their knowledge and consent.
    e. Users will not alter hardware or software setups on the Pampa ISD network or resources without the knowledge and approval of supervisor or the Director of Information Technology.
3. Security
    a. Users are responsible for individual work-related accounts and should take all reasonable precautions to prevent others from being able to use accounts.

    b. Users will immediately notify a supervisor or Director of Information Technology if a possible security problem has been identified.
    c. Users will avoid the inadvertent spread of computer viruses by following virus protection procedures. These procedures include, but are not limited to:
        i. Use of an anti-virus software;
        ii. Never open an unexpected attachment, particularly files with the extension .exe, .vbs, .shs;
        iii. Scan all disks for viruses;
        iv. Perform backups of files

4. Inappropriate Language
    a. Users will not use inappropriate language in any public messages, private messages, and material created for work to be posted on Pampa ISD webpages.
    b. Users will not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language.
    c. Users will not engage in personal attacks, including prejudicial or discriminatory attacks.
    d. Users will not utilize the Pampa ISD network and/or resources to harass another person.
    e. Users will not knowingly or recklessly post false or defamatory information about another person or organization.
5. Respect for Privacy
    a. Users will not forward or post a personal message that was sent to him/her without, first, obtaining permission of the person who sent the message and verifying the message's authenticity.
    b. Users will not post information, including pictures, about another person without their knowledge and consent.
6. Respecting Resource Limits
    a. Users will utilize Pampa ISD network and/or resources for educational and career development activities.
    b. Users will not download large files unless required for job performance.
    c. Users will not post chain letters or engage in spamming. Spamming is sending an annoying or unnecessary message to a large number of people.
    d. The Technology Department may allow limited access to streaming video and audio sites. This access may be terminated for any user if its use is deemed to interfere with user productivity, pre-empt any business activity, or consume more than a trivial amount of resources. This includes, but is

not limited to, things such as listening to the radio through the internet, stock market tickers, etc.

7. Plagiarism and Copyright Infringement
    a. Users will not plagiarize works that are found on the Internet or on the computers at the work place.
    b. Users will respect the rights of copyright owners. Copyright infringement occurs when a user inappropriately reproduces a work that is protected by copyright. If a work contains language that specifies appropriate use of that work, user will follow the expressed requirements. If the user is unsure whether or not he/she may use a work, the user will request permission from the copyright owner.
    c. Users will not install software on Pampa ISD computers that has not been purchased or approved by Pampa ISD without prior permission of supervisor or designee. A copy of the software media license will be given to the Director of Information Technology for security and auditing purposes.
8. Inappropriate Access to Material
    a. Users will not utilize Pampa ISD network resources, including computers, to access material that is profane or obscene (pornography), that advocates illegal acts, or that advocates violence or discrimination toward other people, unless it specifically states in job description and/or assigned duties.
    b. If users mistakenly access inappropriate information, they will immediately alert supervisor or designee.

Revision History

Date of Change	Author	Rationale
11/14/2019	Dennis Boyd & Melody Baker	Initial implementation
1/21/2020	Dennis Boyd & Melody Baker	Removed inconsistent wording

Email Procedures

Overview

Email is a critical mechanism for business communications at Pampa ISD. However, use of Pampa ISD electronic mail and services are a privilege, not a right, and therefore must be used with respect and in accordance with the goals of Pampa ISD.

Purpose

The purpose of this Email Procedure is to outline appropriate and inappropriate use of Pampa ISD email systems and services in order to minimize disruptions to services and activities, as well as comply with applicable policies and laws.

Scope

The scope of these procedures applies to all email systems and services owned by Pampa ISD, all email account users at Pampa ISD (both temporary and permanent), and all company email records.

Procedures

General Expectations of End Users

a. Important official communications are often delivered via email. As a result, employees of Pampa ISD with email accounts are expected to check their email in a consistent and timely manner so they are aware of important announcements and updates, as well as for fulfilling business and role-oriented tasks.
b. Email users are responsible for mailbox management, including organization and cleaning. If a user subscribes to a mailing list, he/she must be aware of how to remove himself/herself from the list and is responsible for doing so in the event that their current email address changes.
c. Email users are also expected to comply with normal standards of professional and personal courtesy and conduct.

Appropriate Use

Individuals at Pampa ISD are encouraged to use email to further the goals and objectives of Pampa ISD. The types of activities that are encouraged include:

a. Communicating with peers, business partners of Pampa ISD, and clients within the context of an individual's assigned responsibilities.
b. Acquiring or sharing information necessary or related to the performance of an individual's assigned responsibilities.
c. Participating in educational or professional development activities.

Inappropriate Use

a. Pampa ISD email systems and services are not to be used for purposes that could be reasonably expected to cause excessive strain on systems.
b. Individual email use will not interfere with others' use and enjoyment of Pampa ISD email system and services.
c. Email use at Pampa ISD will comply with all applicable laws, all Pampa ISD policies, and all Pampa ISD contracts.

The following activities are deemed inappropriate uses of Pampa ISD systems and services and are prohibited.

a. Sending or forwarding offensive and/or inappropriate emails.
b. Use of email for illegal or unlawful purposes, including copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, soliciting for illegal pyramid schemes, and computer tampering (e.g., spreading computer viruses).
c. Use of email in any way that violates Pampa ISD policies, rules, or administrative orders including, but not limited to, board policies, administrative policies and procedures, etc.
d. Viewing, copying, altering, or deleting email accounts or files belonging to Pampa ISD or another individual without authorized permission.
e. Sending of unreasonably large email attachments. The total size of an individual email message sent (including attachment) should not exceed 25 Mb.
f. Opening email attachments from unknown or unsigned sources. Attachments are the primary source of computer viruses and should be treated with utmost caution.
g. Sharing email account passwords with another person or attempting to obtain another person's email account password. Email accounts are to only be used by the registered user.
h. Excessive personal use of Pampa ISD email resources. Pampa ISD allows limited personal use for communication with family and friends, independent

learning, and public service so long as it does not interfere with user productivity, pre-empt any business activity, or consume more than a trivial amount of resources. Pampa ISD prohibits personal use of its email systems and services for unsolicited mass mailings, non-Pampa ISD commercial activity, political campaigning, dissemination of chain letters, and use by anyone who has not been authorized by the Technology Department.

Monitoring and Confidentiality

a. The email systems and services used at Pampa ISD are owned by Pampa ISD and are, therefore, its property. This gives Pampa ISD the right to monitor any and all email traffic passing through its email system. If Pampa ISD discovers or has good reason to suspect activities that do not comply with applicable laws or this policy, email records may be retrieved and used to document the activity. While Pampa ISD does not actively read end-user email, email messages may be inadvertently read by IT staff during the normal course of managing the email system.
b. In addition, backup copies of email messages may exist, despite end-user deletion, in compliance with Pampa ISD records retention policy. The goals of these backup and archiving procedures are to ensure system reliability and prevent business data loss.
c. Use extreme caution when communicating confidential or sensitive information via email. Keep in mind that all email messages sent outside of Pampa ISD become the property of the receiver. A good rule is to not communicate anything you wouldn’t feel comfortable being made public. Demonstrate particular care with using the “Reply” command during email correspondence.

Reporting Misuse

If a user receives an offensive and/or inappropriate email, do not forward, delete, or reply to the message. Instead, report it to a supervisor or designee.

Disclaimer

Pampa ISD assumes no liability for direct and/or indirect damages arising from the user’s use of Pampa ISD email system and services.

Revision History

Date of Change	Author	Rationale

11/14/2019	Dennis Boyd & Melody Baker	Initial implementation

Physical Access Procedures

Overview

Technical support staff, security administrators, system administrators, and others may have Technology Department physical facility access requirements as part of their job responsibilities. The granting, controlling, and monitoring of the physical access of Technology Department facilities is extremely important to an overall security program.

Purpose

The purpose of the Physical Access Procedures is to establish the rules for granting, controlling, monitoring, and removal of physical access to Technology Department facilities.

Scope

The scope of these procedures applies to all technical support staff, security administrators, system administrators, and any others that may require access to Technology Department physical facilities as part of job responsibilities.

Procedures

- All physical security systems must comply with all applicable regulations such as, but not limited to, building codes and fire prevention codes.
- Physical access to all Technology Department restricted facilities must be documented and managed.
- All Technology Department facilities must be physically protected in proportion to the criticality or importance of their function at Pampa ISD.
- Access to Technology Department facilities must be granted only to Pampa ISD support personnel and contractors whose job responsibilities require access to that facility.

- Visitors, including approved contractors, must be escorted in access-controlled areas of Technology Department facilities.
- The process for granting card, code and/or key access to Technology Department facilities must include the approval of the person responsible for the facility.
- Each individual that is granted access rights to a Technology Department facility must sign the appropriate confidentiality agreement.
- Requests for access must come from the applicable Pampa ISD data/system owner.
- Access cards, codes and/or keys must not be shared or loaned to others.
- Access cards, codes and/or keys that are no longer required must be returned to the person responsible for the Technology Department facility. Cards must not be reallocated to another individual bypassing the return process.
- Lost or stolen access cards, codes and/or keys must be reported to the person responsible for the Technology Department facility immediately.
- A service charge may be assessed for access cards and/or keys that are lost, stolen or not returned.
- Access cards and/or keys must not have identifying information other than a return mail address.
- All Technology Department facilities that allow access to visitors will track visitor access with a sign in/out log.
- Card/Code access records and visitor logs for Technology Department facilities must be kept for routine review based upon the criticality of the information resources being protected. The person responsible for the Technology Department facility must remove the access card, code and/or key access rights of individuals that change roles within Pampa ISD or are separated from their relationship with Pampa ISD.
- The person responsible for the Technology Department facility shall review access records and visitor logs for the facility on a periodic basis and investigate any unusual access.
- The person responsible for the Technology Department facility must review card, code and/or key access rights for the facility on a periodic basis and remove access for individuals that no longer require access.
- Signage for restricted access rooms and locations must be practical, yet minimal discernible evidence of the importance of the location should be displayed.

Revision History

Date of Change	Author	Rationale

11/14/2019	Dennis Boyd & Melody Baker	Initial implementation

Responsible Use Policy

Technology Resources

To prepare students for an increasingly technological society, The Pampa Independent School District ("Pampa ISD" or "District") provides an array of technology resources to its students and staff for educational and administrative purposes. The goal in providing these resources is to promote educational excellence in the District's schools by facilitating resource sharing, innovation, creativity, and communication with the support and supervision of parents, teachers, and staff. The use of these technology resources is a privilege, not a right.

This agreement sets forth the standards governing Pampa ISD staff and student use of those technology resources. This agreement also sets forth the rules under which authorized users may continue their access to and use of the resources. This agreement promotes the ethical, legal, and school-related use of the Pampa ISD Network (“Network”) and ensures Pampa ISD's compliance with the Children's Internet Protection Act. Personal electronic devices will be governed under this agreement when such devices are attached to the Network.

Access to computers brings the potential availability of material that may not be considered to be of educational value into school setting. Pampa ISD firmly believes that the value of information, interaction, and research capabilities available outweighs the possibility that users may obtain material that is not consistent with the educational goals of the District.

District Responsibilities

Pampa ISD's Superintendent, Administrators, Director of Technology, and Teachers will serve to oversee the District's system and will work with the Texas Education Agency, Region 16 Education Service Center, and other agencies as necessary to ensure the safety of all users of the Network and Internet.

The District will establish a process for setting up individual accounts for storage of information, establish procedures for the storage of images, video, and music files, establish training and information as needed, establish a district virus protection process, and coordinate other activities related to the use of the Network.

The District utilizes software designed to block access to certain Internet sites, and to monitor and log all activity of users of the Network, or otherwise act to verify or enforce compliance with District policies and purposes.

Disclaimer

Pursuant to the Children's Internet Protection Act, Pampa ISD uses filtering software to screen Internet sites for offensive material. The goal is to filter pages containing offensive, sexually explicit, and inappropriate material, including, but not limited to the following categories: Adult Content; Nudity; Sex; Gambling; Violence; Weapons; Hacking; Personals/Dating; Lingerie/Swimsuit; Racism/Hate; Obscene/lndecent/Vulgar; and Illegal/Questionable. Innocuous search requests may lead to sites with highly offensive content. Additionally, having an e-mail address may lead to receipt of unsolicited e-mail containing offensive content. With this in mind, Pampa ISD reminds authorized users that accessing the Internet is done at the risk of the user. No filtering software is one hundred percent effective and it is possible that the software could fail. In the event that the filtering software is unsuccessful and children and/or staff gain access to inappropriate and/or harmful material, Pampa ISD will not be liable. To minimize these risks, staff and student use of the Network is governed by this agreement. Furthermore, staff and students are responsible for seeking assistance in the event they need help in safely conducting Internet searches.

Definition of District Technology Resources

The District's computer systems and networks include any configuration of hardware and software. The systems and networks include all of the computer hardware, operating system software, application software, stored text, and data files. This includes electronic mail, local content, externally accessed content (such as the Internet), optical media, digital images, digitized information, communications technologies, and new technologies as they become available. The District reserves the right to monitor/review all technology resource activity.

General Provisions

Authorized Users

All authorized users shall adhere to the provisions of this agreement (and any other applicable District policy, regulation or administrative directive) as a condition for continued use of the Network. It is a general policy of Pampa ISD to promote the use of computers in a manner that is responsible, legal and appropriate. This agreement is enacted anytime there is a connection to the District's hardwired or wireless network or from any outside line such as Fiber, T-1, BRI, PRI, VPN, Dialup, DSL, Distance Learning Equipment, Cellular Service and other personal electronic devices.

Terms and Conditions for Use of the Pampa ISD Network

Acceptable Uses

Pampa ISD staff and students may use the various resources provided by the Network to pursue educationally-related activities consistent with the District's mission and goals. Commercial use of the District's system is strictly prohibited.

The District will make training available to all users in the proper use of the system and a copy of the responsible use guidelines is available in the Pampa ISD Employee Handbook, the Student Code of Conduct and on the Pampa ISD website. All training in the use of the District's system will emphasize the ethical use of this resource.

Teachers and other staff should help guide students in their use of the Network so that students will learn how Internet resources such as discussion boards, wikis, and blogs can provide valuable educational information from classrooms, schools, and other national and international sources. In addition to using the Network strictly for educational pursuits, authorized users will be expected to follow generally accepted rules of digital citizenship and network etiquette (also known as netiquette). These include, but are not limited to, the following:

1. Use appropriate language.
2. Do not pretend to be someone else when sending or receiving messages.
3. Do not submit, publish, or display any defamatory, inaccurate, racially offensive, abusive, obscene, profane, sexually-oriented, or threatening materials or messages either public or private.
4. Never reveal personal information such as addresses or phone numbers of users or others with their knowledge or consent, or if not required to do so by law or duty.
5. Never use the network in such a way that would disrupt the use of the network by other users.
6. Be polite.

7. Follow existing copyright laws, copies of which may be found in each campus library.
8. Post only allowable Podcasts, Blogs, Forums, WIKIs and Streaming Media. Allowable items:
    a. Support district goals and/or supports the Pampa ISD approved curriculum.
    b. Are student or teacher-created.
    c. Are loaded on a district's website or district approved resource.
9. Use only Applications (Apps) that:
    a. Support of district goals and/or the Pampa ISD approved curriculum.
    b. Are not disruptive to district systems or applications.
    c. Do not incur unauthorized charges.
10. Electronic Mail provides a powerful and nearly instantaneous way to communicate and collaborate with people around the world.
    a. Students may be granted e-mail access only through a district approved e-mail system.
    b. District employees will be provided with an individual e-mail account.
        i. While most people consider e-mail to be private, users of E-mail should clearly understand that the level of privacy afforded is actually much lower than for postal correspondence. Pampa ISD reserves the right to review all e-mail as it deems appropriate, including for purposes of enforcing adherence to the guidelines for use set forth in this Agreement, other District policies, or other legal requirements.
        ii. The District is providing e-mail access for the purpose of furthering its educational mission. It is expected that members of the school community will make use of that access for educational purposes. Commercial use of the District's e-mail access or other electronic communications access is not permitted.

Unacceptable Uses

Unacceptable uses of the Network include, but are not limited to:

1. Downloading or installing unauthorized games, programs, files, electronic media, and/or stand-alone applications from the Internet or placing external data on any computer, whether stand-alone or networked to the District's system, without permission from the Technology Department.
2. Attempting to log on or logging on to a computer or e-mail system by using another's password. Assisting others in violating this rule by sharing information or passwords is also unacceptable.

3. Attempting to bypass the district's telecommunication system through the use of software, hardware or outside proxy systems. Assisting others in violating this rule by sharing information or passwords is also unacceptable.
4. Bypassing district network security by connecting a district device to an external network, including cellular service (e.g.-hot spot, tethering, etc.), or any other method while on Pampa ISD property.
5. Improper use of any computer or the network. This includes the following:
    a. Submitting, publishing, or displaying any defamatory, inaccurate, racially offensive, abusive, obscene, profane, sexually-oriented, or threatening materials or messages, either public or private, to teachers, students, parents, or other individuals or groups.
    b. Using the network for cyber-bullying
    c. Using the network for financial gain, political, or commercial activity.
    d. Attempting to harm or harming equipment, materials, or data.
    e. Attempting to send or sending anonymous messages of any kind.
    f. Using the network to access inappropriate material.
    g. Knowingly placing a computer virus on a computer or the network.
    h. Using the network to provide addresses or other personal information that others may use inappropriately.
    i. Accessing information resources, files, and documents to which you have not been granted access or without authorization from another user.
6. Using inappropriate or impolite language.
7. Disclosing personal information, including the names, addresses, and telephone numbers of students or colleagues. If a Pampa ISD employee receives a Public Information Act Request or Freedom of Information Act Request, the request must be immediately forwarded to the Superintendent.
8. Intentionally disrupting the use of the Network for other users, including, but not limited to, disruptive use of any processes or programs, utilizing tools for ascertaining passwords, participating in or commissioning a Distributable Denial of Service (DDoS) attack, or engaging in "hacking" of any kind.
9. Intentionally spreading computer viruses or programs that loop repeatedly, or for the purpose of infiltrating a computer system without authorization or for damaging or altering the software components of a computer or computer system.
10. Disclosing the contents or existence of Pampa ISD computer files, confidential documents, e-mail correspondence, or other information to anyone other than authorized recipients.
11. Attempting to harm or destroy Pampa ISD equipment or materials, data of another user of the District's system, or any of the agencies or other networks to which the District has access.

System Access

Access to the District's network systems will be governed as follows:

1. Student and staff members are the only authorized user of their assigned device.
2. Students and staff members will have access to the District's resources for class assignments and research.
3. Students and staff members will be responsible for the integrity of their accounts by keeping passwords confidential and will not allow another user access to their account.
4. Any system user identified as a security risk or having violated the Responsible Use Agreement may be denied access to the District's system. Other consequences including discipline or adverse employment action, as applicable may also occur. See "Sanctions" below.
5. Any system user having been denied access rights may be reinstated with a limited access account to reduce the level of security risk to the system. Limits on this type of account may include time limitations, station access limitations, file access restrictions, and a revocation of Internet access privileges.
6. Personal devices may only be connected to the district network via wired or wireless connection with express permission from the technology department and may not be used as a replacement or in lieu of district provided devices.
7. Student and staff members may be allowed network access using their personal devices. This access may be revoked at any time by the Technology Department.

Campus Level Responsibilities

The campus principal or designee will:

1. Be responsible for disseminating, collecting signed permission forms, and enforcing the Responsible Use Agreement.
2. Ensure that employees supervising students who use the District's systems provide information emphasizing the appropriate and ethical use of this resource.

Individual User Responsibilities

The following standards will apply to all users of the District's computer network systems:

1. The user in whose name a system account is issued will be responsible at all times for its proper use. If a user feels that a password has been compromised, the user is responsible for immediately making a report to an administrator.
2. The system may not be used for illegal purposes, in support of illegal activities, or for any other activity prohibited by district guidelines.

3. Users may not use another person's system account.
4. Any App purchased with a Pampa ISD account will become the property of Pampa ISD.
5. Users, if granted access to electronic mail, are asked to archive or delete electronic mail consistent with the District's retention policies.
6. Users are asked to delete unneeded files from the District servers on a regular basis.
7. Users will be responsible for the care and condition of their computer systems.
8. Maintenance issues should be reported to the Technology Department using the established procedures.
9. School issued devices should never be taken to an outside service repair provider. All repairs must be done through the authorization of the Technology Department.

Users will be responsible for following all copyright laws and terms of service, including but not limited to personal subscriptions to Netflix, Amazon Prime Video, Hulu and all other media.

All authorized users are to promptly report any breaches of security, violations of responsible use, (including inadvertent access to prohibited sites), and the transmission of web addresses or e-mail information containing inappropriate material to the campus principal or Pampa ISD Technology staff member. Failure to report any incident promptly may subject the authorized user to corrective action consistent with the Disciplinary Code, District policies, or applicable directives.

Intentional attempts to degrade or disrupt system performance may be viewed as violations of Pampa ISD guidelines and, possibly, as criminal activity under applicable state and federal laws, including the Texas Penal Code, Computer Crimes, Chapter 33. This includes, but is not limited to uploading or creating of computer viruses, system break-in utilities, DDoS attacks, or system hacking programs. Vandalism as defined above will result in the cancellation of system use privileges and possible criminal prosecution. The party will be responsible for restitution of costs associated with system restoration, hardware, or software costs.

Authorized User Websites

The district will establish a Web site and will develop Web pages that will present information about the district. The district will have a designated Webmaster, responsible for maintaining the District Web site.

Schools and classes are encouraged to establish Web pages that present information about the school or class activities. The building principal or designee will be responsible for managing the school Web site. All sites must be for educational purposes.

Only authorized users may create web pages as a part of a campus or class activity.

Material presented on an authorized users' website must meet the educational objectives of the class activity. Pampa ISD reserves the absolute right to exercise control over the content and/or style of the authorized users' web pages.

Only those students whose parent(s) or guardian(s) have completed the Consent and Release Form may post their work or picture on student or school websites. Students whose work, likeness (as captured by photograph, video or other media) or voices are presented on a student website shall be identified by first name only for confidentiality and safety purposes.

Monitoring

The Network is routinely monitored to maintain efficiency. Authorized users should be aware that use of the Network, including e-mail, is subject to monitoring by the Pampa ISD Technology Department and designated administrators. Any activities related to or in support of violations of this agreement (or other District policy) may be reported and will subject the user to sanctions specified either in the Student Code of Conduct, this agreement, other applicable District policy, or administrative directives.

Assumption of Risk

Pampa ISD will make a good faith effort to keep the Network system and its available information accurate. However, authorized users acknowledge the following:

- There is no warranty of any kind, either express or implied, regarding the accuracy, quality, or validity of any of the data or information available.
- Pampa ISD is not liable for lost or corrupted data. While Pampa ISD utilizes backup software, users are encouraged to safeguard important files.
- Pampa ISD does not warrant that the Network will be error free or free of computer viruses.
- Pampa ISD is not responsible for any damage, physical or software based, that is incurred to personal devices while connected to the Network.
- In making use of these resources, authorized users agree to release Pampa ISD from all claims of any kind, including claims for direct or indirect, incidental, or consequential damages of any nature, arising from any use or inability to use the network, and from any claim for negligence in connection with the operation of the Network.
- The information available through the Internet may be inaccurate. Pampa ISD has no ability to maintain such information and has no authority over these

materials. Pampa ISD makes no warranty of any kind, either express or implied, regarding the accuracy, quality, or validity of the data and/or information residing on or passing through the Network from outside networks.

- Use of the Network is at the risk of the authorized user.

Social Media Policy

Social media is a communication tool in the form of websites or applications that staff and students use to share information and exchange ideas. Pampa ISD understands the value of social media and encourages its use with the understanding that guidelines will be in place to protect district approved accounts/pages.

Users are responsible for their own behavior when communicating with social media. They will be held accountable for the content of the communications that they state/post on social media. Users are responsible for complying with the School District employee, student and conduct policies. Users may not disrupt the learning atmosphere, educational programs, school activities, and the rights of others.

The School District has the right, but not the duty, to inspect, review, retain, or remove electronic communication created, sent, displayed, received or stored on and over the School District network and to monitor, record, check, track, log, access or otherwise inspect its network system.

The School District is not held accountable for any content published using a personal social media account.

Social Media Guidelines – Staff

Any employee wishing to create a social media account/page for district resources is responsible for obtaining permission from your campus administrator.

- Request must be submitted through Eduphoria Formspace
- All content must be moderated by requestor or campus approved delegate

Any employee publishing content to a district approved social media account/page agrees not to:

- Post material that Pampa ISD determines is threatening, harassing, illegal, obscene, defamatory, slanderous, or hostile to any individual or entity.
- Post phone numbers, email addresses or other confidential information of students, faculty, or any other person other than yourself. If you choose to post your own contact information for any reason, please be aware that the information will be available to the public and is, therefore subject to misuse.

- Post material that infringes on the rights of Pampa ISD or any individual or entity, including private, intellectual property or publication rights.
- Post material that promotes or advertises a commercial product or solicits business or membership or financial or other support in any business, group or organization except those which are officially sponsored by Pampa ISD, except in designated areas specifically marked for this purpose.
- Post chain letters, post the same comment multiple times, or otherwise distribute “spam” via Pampa ISD sponsored site.
- Allow any other individual or entity to use your identification for posting or viewing comments.
- Post comments under multiple names or using another person’s name.

It is the employee responsibility to ensure permission has been granted by the parent/guardian before posting a photo on a social media page.

For information regarding private communication using electronic media see Policy DH in the Employee Handbook.

Social Media Guidelines – Student

This Administrative Regulation applies to all School District environments, whether the social media is used on School District property, or beyond School District property (including but not limited to, at a third-party’s contracted property).

In addition to the regulations provided in the School District’s Social Media Policy, some guidelines include but are not limited to the following. The School District reserves the right to determine if any guideline not appearing in the list below constitutes acceptable or unacceptable social media use.

- Students must not promote or appear to promote illegal drugs, illegal activities, violence, drinking, and cyber bullying.
- Students must not impersonate or access another user’s account/page with or without permission.
- Students should state/post only what they want the world to see. Imagine your parents, teachers, and administrators visiting your social media. Essentially, once a student shares something it is likely available after (s)he removes it from the social media and could remain on the internet permanently.
- Students should comply with the rules that have been established for the School District’s educational social media when they us it.

Indemnification

The authorized user indemnifies and holds Pampa ISD harmless from any claims, including attorney's fees, resulting from the user's activities while utilizing the Network that cause direct or indirect damage to the user, Pampa ISD, or third parties.

Sanctions

Students

Failure to abide by this agreement may subject the authorized Student user to corrective action ranging from suspension of some or all access privileges up to and including expulsion and prosecutions according to the Student Code of Conduct.

- If access to the Network is revoked by a school faculty member the Student user has the right to appeal the revocation within thirty (30) days, in writing, to the principal of the school.
- If access to the Network is suspended by the Pampa ISD Technology Department, the Student user may appeal the suspension to the Superintendent or designee.
- Once an authorized user is removed from the Network, there shall be no obligation to provide a subsequent opportunity to access the Network.

Employees

Failure to abide by this agreement and other related policies or administrative directives may subject the authorized Employee user to corrective action, ranging from a reprimand, denial of access to the Network, or adverse employment action (up to and including termination of employment). Once an authorized Employee user is removed from the Network, there shall be no obligation to provide a subsequent opportunity to access the Network.

Revision History

Date of Change	Author	Rationale
7/1/2019	Dennis Boyd & Melody Baker	Annual Review