Kermit Independent School District
Employee Guidelines for
Responsible Use of Technology Resources
(Acceptable Use Policy or AUP)

Kermit Independent School District uses technology as one way of enhancing the mission to teach the skills, knowledge, and behaviors student will need to succeed in today's world. KISD makes a variety of communications and information technologies available to students through computer/network/Internet access. These technologies, when properly used, promote educational excellence in the District by facilitating resource sharing, innovation, and communication. These resources may include various educational computer programs, productivity software, online assessment tools, and other materials. Resources may be accessed via local computers or other devices, through the Kermit ISD local area network, or via the Internet (World Wide Web).

With this educational opportunity comes responsibility. In order for the District to be able to continue to make its technology resources available, all users must take responsibility for appropriate and lawful use of this access. It is important that you read the District policy, administrative regulations, and agreement form and ask questions if you need help in understanding them. Inappropriate system use may result in the loss of the privilege to use this educational tool. Illegal, unethical or inappropriate use of these technologies can have dramatic consequences; harming the District, its students and its employees. These Responsible Use Guidelines are intended to minimize the likelihood of such harm by educating District users and setting standards which will serve to protect the District and students. It will be each user's responsibility to follow the rules for appropriate and acceptable use. The District firmly believes that digital resources, information and interaction available on the computer/network/Internet far outweigh any disadvantages.

GENERAL GUIDELINES:

Definition of District Technology System:

The District's computer systems and networks (system) are any configuration of hardware and software. The system includes but is not limited to the following:

- Telephones, cellular telephones, and voicemail technologies;
- Email accounts;
- Servers;
- Computer hardware and peripherals;
- Software including operating system software and application software;
- Digitized information including stored text, data files, email, digital images, and video and audio files;
- Internally or externally accessed databases, applications, or tools (Internet- or District-server based);
- District-provided Internet access;
- District-filtered public Wi-Fi; and
- New technologies as they become available.

Use & Care of District Technology Devices:

- If you are being issued or allowed to use a District technology device, you will be given additional materials addressing the proper use, care, and/or return of these devices.
- If you utilize school District equipment and/or software outside of the District, you must still follow the Kermit ISD Technology AUP rules while utilizing the school District's resources. (example: if you take a laptop home or offsite and access the internet, it is forbidden to surf for porn, gambling, etc.)
- Modifying or changing computer settings and/or internal or external configurations without appropriate permission is prohibited.

- **Vandalism/Mischief:**
    - Any malicious attempt to harm or destroy District equipment, materials or data;, or the malicious attempt to harm or destroy data of another user of the District's system, or any of the agencies or other networks to which the District has access is prohibited.
    - Deliberate attempts to degrade or disrupt system performance are violations of District policy and administrative regulations and may constitute criminal activity under applicable state and federal laws. Such prohibited activity includes, but is not limited to, the uploading or creating of computer viruses.
    - Vandalism as defined above is prohibited and may result in the cancellation of system use privileges, and other disciplinary measures.

Access to Computer/Network/Internet:

- **Privilege:** Access to the District's computer/network/Internet is a privilege, not a right. The District reserves the right to regulate, control, suspend or deny that privilege.
- **Restrictions:** Each District computer and public Wi-Fi (available for users who bring their own personal telecommunication devices) has filtering software that blocks access to visual depictions that are obscene, pornographic, inappropriate for students, or harmful to minors, as defined by the federal Children's Internet Protection Act (CIPA). Filtered Internet access is provided to students as defined by CIPA. For more information, or more specific guidelines, please refer to CQ(LOCAL) and CQ(LEGAL) on file in the front offices on all campuses or via the KISD website. Other activities may be restricted based upon their perceived educational value, such as gaming sites.

Use of Personal Telecommunication Devices:

- The District believes technology is a powerful tool that enhances learning and enables users to access a vast amount of academic resources. The District's goal is to increase access to digital tools and facilitate immediate access to technology-based information.
- The District provides a filtered, wireless network through which users may be able to connect privately owned (personal) telecommunication devices, as allowed by campus and classroom policies and procedures.
- Users using personal telecommunication devices must follow the recommended guidelines and policies while on school property, attending any school-sponsored activity, or using the Kermit ISD network. See the KISD Board Policy, District Employee Handbook, and district BYOD guidelines for specific guidelines.

Accessing District Internet, Email, or Other District Resources via Cellular Phone or other Handheld Communication Device:

- Employees who choose to access the District's Internet or their own District email accounts on their personal handheld communication device (e.g., cell phone, Palm Pilot, etc.) may do so subject to the following restrictions and requirements.
- The same standards of proper and professional use of the District Internet and District email system apply (including the entirety of this Policy, as well as any provisions applicable from Board Policy (CQ (LEGAL), CQ (LOCAL)), or Employee Handbook, and any other applicable rules or policies) regardless of whether the District services at issue are accessed via District computer or personal device.
- Use of personal cell phones or other handheld communication devices for business purposes should be limited. Employees are expected to conduct themselves in a professional manner when corresponding as employees of the District, and failure to do so may result in disciplinary action where the behavior or conduct is school related (example: sending threatening text messages to a coworker from a personal cell phone).
- The District strongly encourages employees who choose to use personal communication devices for business purposes to protect those devices with "password protection", blocking any unauthorized users access to its contents.
- Electronic mail transmissions and other use of the District's electronic communications system by students and employees shall not be considered private. The District reserves the right to monitor access to and use of District email, District Internet, or other network or computer-related activity, engage in routine computer maintenance and housekeeping, carry out internal investigations, prepare responses to requests for public records, or disclose messages, data, or files to law enforcement authorities. Monitoring shall occur at any time to ensure appropriate use.
- **Reminder:** As an employee of a public school district, your communications regarding District business

may be subject to public information act requests. Consider this possibility before sending any communication from a cell phone, or other similar device, which contains information or issues of District business.

Security/Reporting:

- If knowledge of inappropriate material or a security problem on the computer/network/Internet is identified, the user is expected to discontinue the access and to report the incident to the supervising staff member.
- The security problem should not be shared with others.

Subject to Monitoring:

- All District computer/network/Internet usage shall NOT be considered confidential and is subject to monitoring by designated staff at any time to ensure appropriate use.
- Users should not use the computer system to send, receive or store any information, including email messages, that they consider personal or confidential and wish to keep private.
- All electronic files, including email messages, transmitted through or stored in the computer system will be treated no differently than any other electronic file.
- The District reserves the right to access, review, copy, modify, delete or disclose such files for any purpose.
- Users should treat the computer system like a shared or common file system with the expectation that electronic files, sent, received or stored anywhere in the computer system, will be available for review by any authorized representative of the District for any purpose.
- Personal telecommunication devices are subject to examination in accordance with disciplinary guidelines if there is reason to believe that the Responsible Use Guidelines have been violated.

Employee Computer/Network/Internet Responsibilities

District users are bound by all portions of the Responsible Use Guidelines. A user who knowingly violates any portion of the Responsible Use Guidelines will be subject to suspension of access and/or revocation of privileges on the District's system and will be subject to disciplinary action in accordance with the Board-approved policies.

Acceptable Use:

Computer/Network/Internet access will be used to enhance learning consistent with the District's educational goals. The District requires legal, ethical and responsible computer/network/Internet use.

- You will be assigned an individual account, and you are responsible for not sharing the password for that account with others. Pre-K students will be logged on under their teacher's account.
- By accepting your account password and other information from the District and accessing the Network or the Internet, you are agreeing to follow the rules in this Policy.
- You will be held responsible at all times for the proper use of your account, and for any activity that occurs under the use of your account login. If you leave your device or user account unattended and logged in with the device unlocked, and inappropriate activity occurs, you may be held responsible for that activity and Kermit Independent School District may suspend or revoke your access if you violate the rules.
- Users must assume personal responsibility to behave ethically and responsibly, even when technology provides them the freedom to do otherwise.
- All users must use all software in accordance with license agreements and the District's software regulation. All users acknowledge that they do not own this software or its related documentation, and, that unless expressly authorized by the software publisher, may not make additional copies.
- Users must always respect copyrights and trademarks of third-parties and their ownership claims in images, text, video and audio material, software, information and inventions.
- The account is to be used mainly for identified educational purposes, but some limited personal use is permitted. Limited personal use shall be permitted if the use:
    - Imposes no tangible cost to the District;
    - Does not unduly burden the District's computer or network resources;
    - Has no adverse effect on a student's academic performance;
    - And/or is not used in any way for personal gain.

Inappropriate Use

Inappropriate use includes, but is not limited to, those uses that violate the law, those are specifically named as violations in this document, that violate the rules of network etiquette, or that hamper the integrity or security of this computer/network/Internet system or any components that are connected to it. The following actions are considered inappropriate uses, are prohibited, and may result in revocation of the student's access to the computer/network/Internet.

Violations of Law.

- Transmission of any material in violation of any federal or state law is prohibited. This includes, but is not limited to:
  - threatening, harassing, defamatory or obscene material;
  - copyrighted material;
  - plagiarized material;
  - material protected by trade secret; or
  - blog posts, Web posts, or discussion forum/replies posted to the Internet which violate federal or state law.
- Tampering with or theft of components from District systems may be regarded as criminal activity under applicable state and federal laws. Any attempt to break the law through the use of a District computer/network/Internet account may result in prosecution against the offender by the proper authorities. If such an event should occur, the District will fully comply with the authorities to provide any information necessary for legal action.

Inappropriate Uses:

- Using the system for any illegal purpose.
- Downloading or using copyrighted information, without permission from the copyright holder.
- Fraudulently altering or copying documents or files authored by another individual is prohibited (plagiarism).
- Deleting, examining, copying, or modifying files and/or data belonging to other users, without their permission is prohibited
- Intentional or unauthorized access or attempted access of any restricted portion of the District's computer systems, networks, or private databases to view, obtain, manipulate, or transmit information, programs, or codes is prohibited.
- Impersonating another user, attempting to, or actually accessing or using another person's logon, password, or account with or without permission.
- Downloading files, running programs or installing applications without consent from appropriate administrative staff.
- Changing any computer configurations and/or settings without authorization.
- Encrypting communications to avoid security review.
- Disabling or attempting to disable or bypass any Internet filtering device, including the use of VPN or proxy servers and similar methods.
- Use or possession of hacking/cracking type software is strictly prohibited
- Misuse of equipment that could lead to damage, including but not limited to touching LCD screens, unplugging cables, inserting foreign objects into drives, connections or other openings).
- Intentionally introducing a virus or otherwise attempting to harm, disrupt, or disable the computer equipment, programs, material or data.
- Wasting school resources through the improper use of the computer systems. Example: Messenger Services, Internet Radio, Chat/Newsgroups, hate mail, chain letters, harassment, discriminatory remarks and other antisocial behaviors, etc...
- Users may not redistribute or forward confidential information without proper authorization. Confidential information should never be transmitted, redistributed or forwarded to outside individuals who are not expressly authorized to receive the information.
- Revealing personal information about oneself or others such as, but not limited to, home addresses, phone numbers, email addresses, birthdates or of others is prohibited.

- Posting messages or accessing materials that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.
- Verbal or written language that is considered inappropriate in the classroom is also inappropriate in all uses of blogs, wikis, podcasts, and other District-approved digital tools.
- Commercial use of Kermit Independent School District's system.

Consequences of Agreement Violation

Any attempt to violate the provisions of this agreement may result in revocation of the user's access to the computer/network/Internet, regardless of the success or failure of the attempt. In addition, employee disciplinary and/or appropriate legal action may be taken.

Possible Consequences for Inappropriate Use

- Suspension of access to the Internet.
- Suspension of computer/email login account.
- Revocation of the computer/email login account.
- Payment for any intentional damage to district equipment or software.
- Other disciplinary or legal action, in accordance with Board Policy, the Employee Handbook and applicable laws.

Denial, Revocation, or Suspension of Access Privileges. With just cause, the System Administrator and/or building principal, may deny, revoke, or suspend computer/network/Internet access as required, pending an investigation.

KERMIT INDEPENDENT SCHOOL DISTRICT

EMPLOYEE AGREEMENT FOR ACCEPTABLE USE OF THE ELECTRONIC COMMUNICATIONS SYSTEM

I understand that my computer use is not private and that the District will monitor my activity on the computer system.

I have read the District's electronic communications system policy and administrative regulations and agree to abide by their provisions. In consideration for the privilege of using the District's electronic communications system and in consideration for having access to the public networks, I hereby release the District, its operators, and any institutions with which they are affiliated from any and all claims and damages of any nature arising from my use of, or inability to use, the system, including, without limitation, the type of damages identified in the District's policy and administrative regulations.

Signature: _____

Date: _____

Personal Information: (Please print legibly)

Last Name: _____ **First Name:** _____ **Middle:** _____
(Full Legal Name as listed on your Social Security card)

Dept./Grade Level _____

Name you prefer to be called, if different from above:

_____

Please circle your reporting campus
ELEM JH HS COOP AD MNT

Date of Birth: _____

Home Address: _____

_____

Home Phone Number: _____

Cell Phone: _____