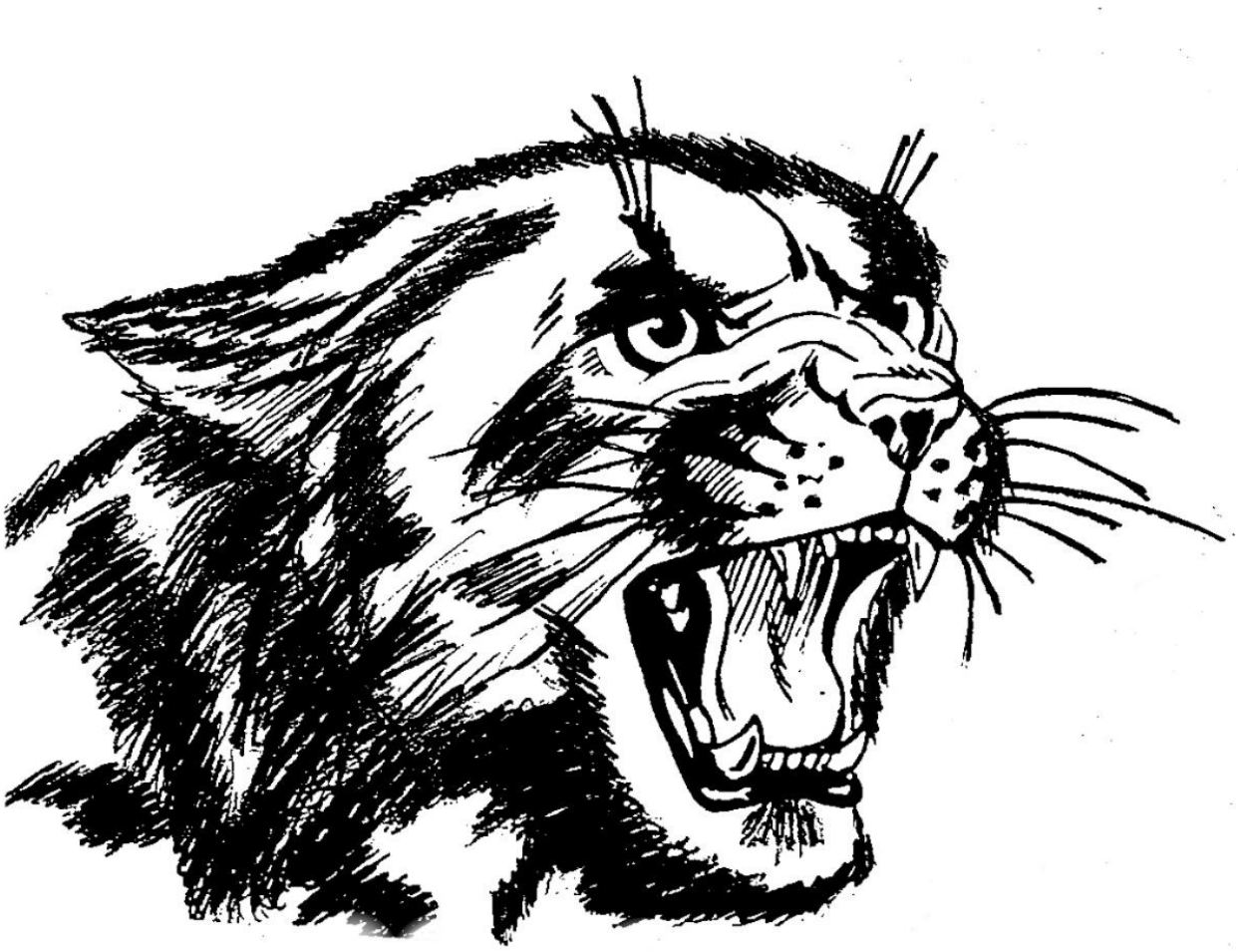
Water Valley ISD



Acceptable Use Policy (Employee) 2023-2024

Acceptable Use Policy
Section I

WATER VALLEY INDEPENDENT SCHOOL DISTRICT
ELECTRONIC INFORMATION SYSTEMS/NETWORK
USER POLICY

Introduction
Water Valley ISD recognizes the need to regulate the acceptable use of technology to control the use of the Internet. The Internet is an electronic highway connecting thousands of computers all over the world and millions of individual subscribers. The District recognizes that the Internet can be used to facilitate many educational activities. The Internet is not meant to replace education, but rather, to facilitate the educational process. It should be used as an adjunct to teaching. The Internet can be a valuable learning tool in the areas of electronic mail, research, data searches, enrichment materials, electronic field trips, and library references. Water Valley ISD resources available on the Internet will allow classroom projects such as pen pal discussions, scientific data collection, and international cultural exchanges. News retrieval services, encyclopedias, scientific and educational databases will be instantaneously accessible to Water Valley students and teachers.

Philosophy
Water Valley ISD believes in the value of incorporating learner-centered experiences in the total educational process. Our philosophy is to make Network/Internet access available to all students, teachers, and staff in Water Valley ISD. Therefore, the District has made Internet-access available to all grade levels because of the many resources it has to offer and the enhanced opportunities for research it provides.

Educational Value Risk
With this access comes the availability of material that may not be considered to be of educational value in the context of the school setting. Sites accessible via the Network/ Internet may contain material that is illegal, defamatory, inaccurate or controversial. Although the District will attempt to limit access to most of this objectionable material, controlling all materials on the Network/Internet is impossible. On a global network, it is impossible to control all materials; an industrious user may discover controversial information. The Water Valley ISD Board of Trustees believes that the valuable information and interaction available on these networks far outweigh the possibility that users may locate material that is not consistent with the educational goals of Water Valley School District.

User Responsibilities
Network/Internet users are responsible for their actions in accessing available resources which are consistent with the educational goals of Water Valley ISD.

Mandatory Training
To educate all users of Internet access through the Water Valley ISD network, mandatory training on proper Network/Internet conduct is required before access will be allowed.

Levels of Access/Teacher Supervision
All students are expected to exercise responsible use of the Network/Internet at all times. Elementary students will have a teacher/aide monitoring their work on the Network/Internet. At junior high, and high school, it is the intent of the district to have personnel present during the students' Network/Internet use; however, due to the nature of their work, it may not always be possible to directly monitor their work. Filtering mechanisms will be used district wide. Sites being accessed by users may be monitored at any time.
Access to the District's electronic communications system will be governed as follows:

1. With the approval of the immediate supervisor, District employees will be granted access to the District's system.

2. The District will require that all passwords be changed periodically at the discretion of the Technology Director or designee.

3. Any system user identified as a security risk or having violated District and/or campus computer-use guidelines may be denied access to the District's system.

Acceptable Use
Network/Internet access shall be used to improve learning and teaching consistent with educational goals of Water Valley ISD. The District expects legal, ethical and acceptable use of the Network/Internet. Acceptable use will be defined by district policy and local campus administration guidelines.

Unacceptable Use
Every Water Valley ISD user has the responsibility to respect and protect the rights of every user in our community and on the Internet in accordance with the laws of Texas and the United States and with rules and guidelines as set by district policy. All users should be aware that the unacceptable use of electronic information resources can be a violation of local, state, and federal laws. Violations can lead to prosecution. Students are expected to use moral and ethical guidelines in making value decisions regarding network use. Using the network is a privilege, not a right, and the privilege may be revoked at any time for unacceptable conduct. The building principal will make the final determination as to what constitutes unacceptable conduct.

Unacceptable conduct includes, but is not limited to, knowingly engaging in any of the following:
1. Using the network for any illegal activity.
2. Violating software copyright or other contracts, including sharing commercial software.
3. Using the network for financial or commercial gain.
4. Degrading or disrupting equipment or system performance.
5. Vandalizing the data of another user.
6. Wastefully using finite resources.
7. Gaining unauthorized access to resources or entities.
8. Invading the privacy of individuals.
9. Using an account owned by another user without authorization.
10. Posting personal communications without the author's consent.
11. Posting anonymous messages.
12. Placing of unlawful information and/or inappropriate material on a system, or receiving inappropriate material without reporting to staff.
13. Using for product advertisement.
14. Using for political lobbying.
15. Using abusive or otherwise objectionable language in either public or private messages.
16. Sending of messages that are likely to result in the loss of recipients' work or systems.
17. Sending of "Chain letters", or "broadcast" messages to lists or individuals, and any other types of use which would cause congestion of the networks or otherwise interfere with the work of others.
18. Installing, without appropriate approval, software or applications onto computers which access the electronic network.
19. Downloading and/or printing of unauthorized material

DISTRICT TECHNOLOGY DIRECTOR RESPONSIBILITIES

The District Technology Director for the electronic communications system will:

1. Be responsible for disseminating and enforcing applicable District policies and acceptable use guidelines for the District's system at the campus level.

2. Ensure that all users of the District's system complete and sign an agreement to abide by District policies and administrative regulations regarding such use. All such agreements will be maintained on file in the principal's office.

3. Ensure that employees supervising students who use the District's system provide training emphasizing the appropriate use of this resource.

4. Be authorized to monitor or examine all system activities, including electronic mail transmissions, as deemed appropriate to ensure proper use of the system.

5. Be authorized to establish a retention schedule for messages on any electronic bulletin board and to remove messages posted locally that are deemed to be inappropriate.

6. Set limits for disk utilization on the system, as needed.

INDIVIDUAL USER RESPONSIBILITIES

The following standards will apply to all users of the District's electronic information/communications systems:

ON-LINE CONDUCT

1. The individual in whose name a system account is issued will be responsible at all times for its proper use.

2. The system may not be used for illegal purposes, in support of illegal activities, or for any other activity prohibited by District policy.

3. System users may not use another person's system account without written permission from the District Administrator or District Technology Director, as appropriate.

4. System users must purge electronic mail in accordance with established retention guidelines, (The Policy for Records Management Requirements for Electronic Mail is in Appendix B).

5. System users may redistribute copyrighted programs or data only with the written permission of the copyright holder or designee. Such permission must be specified in the document or must be obtained directly from the copyright holder or designee in accordance with applicable copyright laws, District policy, and administrative regulations.

6. System users may upload public domain programs to the system. System users may also download public domain programs for their own use or may non-commercially redistribute a public domain program. System users are responsible for determining whether a program is in the public domain.

7. The signatures on this document are legally binding and indicate that those who signed have read the terms and conditions carefully and understand their significance.

VANDALISM PROHIBITED

Any malicious attempt to harm or destroy District equipment or materials, data of another user of the District's system, or any of the agencies or other networks that are connected to the Internet is prohibited. Deliberate attempts to degrade or disrupt system performance may be viewed as violations of District policy and administrative regulations and, possibly, as criminal activity under applicable state and federal laws. This includes, but is not limited to, the uploading or creating of computer viruses.

Vandalism as defined above will result in the cancellation of system use privileges and will require restitution for costs associated with system restoration, hardware, or software costs.

FORGERY PROHIBITED

Forgery or attempted forgery of electronic mail messages is prohibited. Attempts to read, delete, copy, or modify the electronic mail of other system users or deliberate interference with the ability of other system users to send/receive electronic mail is prohibited.

INFORMATION CONTENT/THIRD PARTY SUPPLIED INFORMATION

System users and parents of students with access to the District's system should be aware that use of the system may provide access to other electronic communications systems in the global electronic network that may contain inaccurate and/or objectionable material.

A student knowingly bringing prohibited materials into the school's electronic environment will be subject to a suspension and/or a revocation of privileges on the District's system and will be subject to disciplinary action in accordance with the Student Code of Conduct.

An employee knowingly bringing prohibited materials into the school's electronic environment will be subject to disciplinary action in accordance with District policies.

DISTRICT WEB SITE

The District will maintain a District Web site for the purpose of informing employees, students, parents, and members of the community of District programs, policies, and practices. Requests for publication of information on the District Web site must be directed to the designated Site Director. The Technology Director and the District Web Site Director will establish guidelines for the development and format of Web pages controlled by the District.

No personally identifiable information regarding a student will be published on a Web site controlled by the District where a 'Denial Form' has been filled out and made available to the Web Site Director in the Principal's office.

No commercial advertising will be permitted on a Web site controlled by the District.

PERSONAL WEB PAGES

District employees, Trustees, and members of the public will not be permitted to publish personal Web pages using District resources.

NETWORK ETIQUETTE

System users are expected to observe the following network etiquette:

1. Be polite. Messages typed in capital letters are the computer equivalent of shouting and are considered rude.

2. Use appropriate language. Swearing, vulgarity, ethnic or racial slurs, and any other inflammatory language are prohibited.

3. Pretending to be someone else when sending/receiving messages is considered inappropriate.

4. Transmitting obscene messages or pictures is prohibited.

5. Revealing personal addresses or phone numbers of the user or others is prohibited.

6. Using the network in such a way that would disrupt the use of the network by other users is prohibited.

TERMINATION/REVOCATION OF SYSTEM USER ACCOUNT

The District may suspend or revoke a system user's access to the District's system upon violation of District policy and/or administrative regulations regarding acceptable use.

Termination of an employee's account or of a student's access will be effective on the date the principal or District Technology Director receives notice of student withdrawal or of revocation of system privileges, or on a future date if so specified in the notice.

ELECTRONIC DEVICES NOT PERMITTED AT SCHOOL:

Computer Laptops, Cell Phones, Radios, CD/DVD players, Game players, iPods and other Electronic Devices.

From an Educational perspective, the items above primarily present another disruption to the educational environment on a day-to-day basis. School disruptions can come in a number of forms. Ringing cell phones can disrupt classes and distract students who should be paying attention to their lessons at hand. Text messaging has been used for cheating. And new cell phones with cameras could be used to take photos of exams, take pictures of students changing clothes in gym locker areas, and so on.
WVISD maintains a phone in every classroom for Teachers, Administrators, Crisis Team Members, and other appropriate adults.

Students are not permitted to use such items as Computer Laptops, Telecommunication Devices (with Text Messaging or Camera Capability), Cameras, Pagers, CD/DVD Players, Audio Recorders, Camcorders, Game Players, Games, iPods or Electronic Devices at school, ***unless prior permission has been obtained from the Principal.*** *Without such permission, Teacher's, upon seeing items used, will collect the item and turn it in to the Principal's office.*

A Fee of $15.00 will be assessed prior to the return of any confiscated items.
Confiscated items will not be returned until the $15.00 is paid in full.
Confiscated items may be picked up by Parents or Legal Guardians only.
No student will be allowed to pick up confiscated items unless permission has been obtained from the Principal.

For Safety purposes, the District permits students to possess cell phones. However, Cell phones must remain turned off during the instructional school day.

Any disciplinary action will be in accordance with the Student Code of Conduct.

For certain items, such as Pagers, in which a third party retains a Legal Right of Ownership, the school may charge for releasing the Pager to the Third Party.

Guidelines for Educators Using Social Networking Sites

Social networks are rapidly growing in popularity and use by all ages in society. The most popular social networks are web-based, commercial, and not purposely designed for educational use. They include sites like Facebook, Twitter, LinkedIn, Pinterest, Google Plus+, Tumblr, Instagram, VK, Flickr, Vine, Meetup, Tagged, Ask.fm, MeetMe, Classmates and others. For individuals, social networking sites provide tremendous potential opportunities for staying in touch with friends and family.

Other educational networking sites are also growing in use. These sites are usually restricted to only certain users and not available to the general public. These include resources such as Moodle, educational wikis, professional online communities such as the Classroom2.0 Ning, or district adoptions of online applications such as Google Apps for Education.

As educators we have a professional image to uphold and how we conduct ourselves online helps determine this image. As reported by the media, there have been instances of educators demonstrating professional misconduct while engaging in inappropriate dialogue about their schools and/or students or posting pictures and videos of themselves engaged in inappropriate activity. Some educators feel that being online shields them from having their personal lives examined. But increasingly, how educators' online identities are too often public and can cause serious repercussions.

One of the hallmarks of social networks is the ability to "friend" others – creating a group of others that share interests and personal news. The district strongly discourages teachers from accepting invitations to *friend* students within these social networking sites. When students gain access into a teacher's network of friends and acquaintances and are able to view personal photos, the student-teacher dynamic is altered. Friending students provide more information than one should share in an educational setting. It is important to maintain a professional relationship with students to avoid relationships that could cause bias in the classroom.

For the protection of your professional reputation, the district recommends the following practices:

<u>Friends and friending</u>

- Do not accept students as friends on personal social networking sites. Decline any student-initiated friend requests.

- Do not initiate friendships with students
- Remember that people classified as “friends” have the ability to download and share your information with others.
- If you wish to use networking protocols as a part of the educational process, please work with your administrators and technology staff to identify and use restricted, school-endorsed networking platforms.

Content

- Do not use commentary deemed to be defamatory, obscene, proprietary, or libelous. Exercise caution with regards to exaggeration, colorful language, guesswork, obscenity, copyrighted materials, legal conclusions, and derogatory remarks or characterizations.
- Weigh whether a particular posting puts your effectiveness as a teacher at risk.
- Post only what you want the world to see. Imagine your students, their parents, your administrator, visiting your site. It is not like posting something to your web site or blog and then realizing that a story or photo should be taken down. On a social networking site, basically once you post something it may be available, even after it is removed from the site.
- Do not discuss students or coworkers or publicly criticize school polices or personnel.
- Do not post images that include students.

Security

- Due to security risks, be cautious when installing the external applications that work with the social networking site. Examples of these sites are calendar programs and games.
- Run updated malware protection to avoid infections of spyware and adware that social networking sites might place on your computer.
- Be careful not to fall for phishing scams that arrive via email or on your wall, providing a link for you to click, leading to a fake login page.
- Visit your profile’s security and privacy settings. At a minimum, educators should have all privacy settings set to “only friends”. “Friends of friends” and “Networks and Friends” open your content to a large group of unknown people. Your privacy

and that of your family may be a risk. People you do not know may be looking at you, your home, your kids, your grandkids, - your lives!

Please stay informed and cautious in the use of all new networking technologies.

Electronic Communications and Social Media

- An employee who uses electronic media to communicate with students shall observe the following:
- The employee may use any form of electronic media **except text messaging**. Only a teacher, trainer, or other employee who has an extracurricular activity may use text messaging, and then only to communicate with students who participate in the extracurricular activity over which the employee has responsibility. An employee who communicates with a student using text messaging shall comply with the following protocol:
    - The employee shall include at least one of the student's parents or guardians as a recipient on each text message to the student so that the student and parent receive the same message; and
    - For each text message addressed to one or more students, the employee shall send a copy of the text message to the employee's district e-mail address for the purposes of records retention.

  The employee shall limit communications to matters within the scope of the employee's professional responsibilities (e.g., for classroom teachers, matters relating to class work, homework, and tests; for an employee with an extracurricular duty, matters relating to the extracurricular activity).

Resources

- Should Students and Teachers be Online Friends?, Cheri Lucas
  http://www.education.com/magazine/article/Students_Teachers_Social_Networking/
- A Teachers Guide to Using Facebook, Bernadette Rego
  http://www.scribd.com/doc/16957158/Teachers-Guide-to-Using-Facebook-Read-Fullscreen
- Social Networking Best Practices for Educators,
  http://www.willard.k12.mo.us/co/tech/Document/SocialNetworkBestPractices.pdf

Internet Safety Policy (Protecting Children in the 21st Century)

The district will educate minors about appropriate online behavior. This includes the appropriate online behavior for interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response. The district's website http://www.wvisd.net/Page/56 has the training for teachers as well as for parents to use for educating minors about appropriate online behavior including interacting with other individuals on social networking websites, in chat rooms, and cyberbullying awareness and response.

Technology Protection Measure (Internet Filtering)

The district has selected a technology protection measure (Internet filtering) for use with the district Internet system. The filtering technology will always be configured to protect against access material that is obscene, illegal (i.e. child pornography) and material that is harmful to minors, as defined by the Children's Internet Protection Act. The district or individual schools may, from time to time, reconfigure the filtering software to best meet the educational needs of the district or schools and address the safety needs of the students.

The district technology department will conduct an annual analysis of the effectiveness of the selected filter and will make recommendations to the Superintendent regarding the selection and configuration of the filter.

The filter may not be disabled at any time that students may be using the district Internet system, if such disabling will cease to protect against access to materials that are prohibited under the Children's Internet Protection Act. The filter may be disabled during non-student use time for system administrative purposes.

Filtering technology has been found to inappropriately block access to appropriate material. To ensure that the implementation of the technology protection measure is accomplished in a manner that retains district control over decision making regarding the appropriateness of material for students; does not unduly restrict the educational use of the district Internet system by teachers and students; and ensures the protection students' constitutional right to access to information and ideas, authority will be granted to selected educators to temporarily or permanently unblock access to sites blocked by the filter.

Authority to temporarily unblock access will be granted to building administrators and or his/her designees, and any media specialists or teacher who regularly uses the Internet for instructional purposes who request permission to have such authority. Individuals granted authority to temporarily unblock sites must meet standards for technical proficiency that are deemed necessary to ensure the security of the system. The technology department shall determine such standards.

To temporarily unblock a site, the authorized individual must review the content of the site, outside of the presence of any student, prior to allowing access to the site by a student. Reports of all instances of temporary unblocking will automatically be forwarded to the district technology director.

If an unauthorized individual believes that the blocked site should be permanently unblocked, a recommendation will be forwarded to the district technology director. The district technology director will make a decision to permanently unblock access to the site. A list of all sites that have been permanently unblocked, together with the rationale for making the decision to unblock the site will be forwarded to the superintendent.

A request to unblock process will be established in secondary libraries to allow students to anonymously request that a blocked site be temporarily or permanently unblocked.

DISCLAIMER

The District's system is provided on an "as is, as available" basis. The District does not make any warranties, whether express or implied, including, without limitation, those of merchantability and fitness for a particular purpose with respect to any services provided by the system and any information or software contained therein. The District does not warrant that the functions or services performed by, or that the information or software contained on, the system will meet the system user's requirements, or that the system will be uninterrupted or error-free, or that defects will be corrected.

Opinions, advice, services, and all other information expressed by system users, information providers, service providers, or other third party individuals in the system are those of the providers and not the District.

The District will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the District's electronic communications system.

GOVERNMENT LAWS:
I will use computers in conformity with laws of the United States and the State of Texas. Violations include, but are not limited to, the following:

Criminal Acts – These include, but are not limited to, "hacking" or attempting to access computer systems without authorization, harassing email, cyberbullying, cyberstalking, child pornography, vandalism, and/or unauthorized tampering with computer systems. (A list of Federal statutes from the United States Department of Justice is below as Appendix A).
Libel Laws - Publicly defaming people through the published material on the internet, email, etc…
Copyright Violations - Copying, selling or distributing copyrighted material without the express written permission of the author or publisher (users should assume that all materials available on the Internet are protected by copyright), engaging in plagiarism (using other's words or ideas as your own).

Appendix A – Unlawful Online Conduct and Applicable Federal Laws

The chart below details the type of unlawful online conduct, potentially applicable federal laws, and the section of the Department of Justice with subject-matter expertise. If the subject matter expert is not a section of the Department, but rather another agency, the entry will have an asterisk following its initials. In many cases, prosecutors may also consider whether the conduct at issue is a violation of 18 U.S.C. § 2 (aiding and abetting) or 18 U.S.C. § 371 (conspiracy).

Unlawful Conduct	Applicable Federal Law	DOJ Section
Denial of Service Attacks	18 U.S.C. § 1030(a)(5)(A) (transmission of program, information, code, or command, resulting in damage)	CCIPS
	18 U.S.C. § 1362 (interfering with government communication systems)	CCIPS
Use of Misleading Domain Name	18 U.S.C. § 2252B (using misleading domain name with intent to deceive a person into viewing obscene material or with intent to deceive a minor into viewing harmful material)	CEOS
Password Fraud	18 U.S.C. § 1030(a)(6) (trafficking in computer passwords)	CCIPS
	18 U.S.C. § 1029 (access device fraud)	Fraud/CCIPS
	18 U.S.C. § 1343 (wire fraud)	Fraud
Obscenity	47 U.S.C. § 223(a)(1)(A) (using telecommunications device to make, create, or solicit, and transmit any obscene comment, request, suggestion, proposal, image, or other communication)	CEOS
	18 U.S.C. § 1465 (using interactive computer service for purpose of sale or distribution of obscene material)	CEOS
Piracy and Intellectual Property Theft	17 U.S.C. §§ 1201-1205 (Digital Millennium Copyright Act)	CCIPS
	17 U.S.C. § 506 and 18 U.S.C. § 2319 (criminal copyright infringement)	CCIPS
	18 U.S.C. § 2319A (trafficking in recordings of live musical performances)	CCIPS

Electronic Threats	18 U.S.C. § 875 (transmitting communications containing threats of kidnap or bodily injury) (Hobbs Act)	CTS
	18 U.S.C. § 1951 (interfering with commerce by robbery, extortion, threats or violence) (Hobbs Act)	DSS
Electronic Harassment	47 U.S.C. § 223 (a)(1)(C) (anonymously using telecommunications device to threaten person who receives communication)	CCIPS
	47 U.S.C. § 223 (a)(1)(C) (anonymously using telecommunications device to harass person who receives communication)	CCIPS
	47 U.S.C. § 223(a)(1)(E) (repeatedly initiates communication with a telecommunication device solely to harass person who receives communication)	CCIPS
Interception of Electronic Communications	18 U.S.C. § 2511 (intercepting electronic communications)	CCIPS
	18 U.S.C. § 2701 (accessing stored communications)	CCIPS
	18 U.S.C. § 1030(a)(2) (accessing a computer and obtaining information)	CCIPS
Cyberstalking	18 U.S.C. § 2261A (using any facility of interstate or foreign commerce to engage in a course of conduct that places person in reasonable fear of death or serious bodily injury to person, person's spouse or immediate family) See also Electronic Harassment	DSS
Hate Crimes	Look to civil rights laws and penalty enhancements	Civil Rights
Libel/Slander	Look to civil laws	
Posting Personal Information on a Website (e.g., phone numbers, addresses)	This is not a violation of law. May also be protected speech under First Amendment.	
Invasion of Privacy	See Interception of Electronic Communications	
Disclosure of Private Information	18 U.S.C. § 2511(1)(c) (disclosing intercepted communications)	CCIPS
Spam	18 U.S.C. § 1037 (CAN-SPAM Act)	CCIPS
Spoofing Email Address	18 U.S.C. § 1037 (CAN-SPAM Act)	CCIPS

Appendix B– Policy for Records Management Requirements for Electronic Mail

Texas State Agencies Model Policy for Records Management Requirements for Electronic Mail

SECTION 1. INTRODUCTION

This policy applies to e-mail used within Water Valley ISD and e-mail used conjointly with the Internet, and does not supersede any state or federal laws, or any other agency policies regarding confidentiality, information dissemination, or standards of conduct. Generally, e-mail should be used only for legitimate state business; however, brief and occasional e-mail messages of a personal nature may be sent and received if the following conditions are met.

SECTION 2. GENERAL GUIDELINES

Personal use of e-mail is a privilege, not a right. Abuse of the privilege may result in appropriate disciplinary action. Employees need to keep in mind that all e-mail is recorded and stored along with the source and destination. Management has the ability and right to view employees' e-mail. Recorded e-mail messages are the property of Water Valley ISD and therefore the taxpayers of the State of Texas. Thus, they are subject to the requirements of the Texas Public Information Act and the laws applicable to State records retention. Employees should be aware that when sending an e-mail message of a personal nature, there is always the danger of the employees' words being interpreted as official agency policy or opinion. Therefore, when an employee sends a personal e-mail, especially if the content of the e-mail could be interpreted as an official agency statement, the employee should use the following disclaimer at the end of the message:

"This e-mail contains the thoughts and opinions of (employee name) and does not represent official (Water Valley ISD) policy."

If the content of the e-mail contains sensitive or confidential information the employee may use the following message at the end of the message:

"This message contains information which may be confidential and privileged. Unless you are the addressee (or authorized to receive for the addressee), you may not use, copy or disclose to anyone the message or any information contained in the message. If you have received the message in error, please advise the sender by reply e-mail and delete the message."

SECTION 3. RESTRICTIONS
Personal e-mail should not impede the conduct of state business; only incidental amounts of employee time--time periods comparable to reasonable coffee breaks during the day--should be used to attend to personal matters. Racist, sexist, threatening, or otherwise objectionable language is strictly prohibited. E-mail should not be used for any personal monetary interests or gain. Employees should not subscribe to mailing lists or mail services strictly for personal use. Personal e-mail should not cause the state to incur a direct cost in addition to the general overhead of e-mail.

SECTION 4. POLICY
It is the policy of [Water Valley ISD] to provide for the efficient, economical and effective management of electronic mail records in accordance with Texas Administrative Code (TAC), Chapter 13, Sections 6.91-6.97 (State Agency Bulletin Number One, Electronic Records Standards and Procedures). TAC Chapter 13, Section 6.92(c), provides that the agency head or designated records management officer must administer a program for the management of records created, received, retained, used, or disposed on electronic media.

The [Water Valley ISD] desires to adopt a policy for that purpose and to prescribe guidelines and procedures for the management of electronic mail consistent with the Electronic Records Standards and Procedures and in the interest of cost-effective and efficient recordkeeping, including long-term records retention for the Archives of the State.

SECTION 5. DEFINITIONS
(1) Electronic mail message-A record created or received on an electronic mail system including brief notes, more formal or substantive narrative documents, and any attachments which may be transmitted with the message.
(2) Electronic mail receipt data-Information in electronic mail systems regarding the date and time of receipt of a message, and/or acknowledgment of receipt or access by addressee(s).
(3) Electronic mail system-A computer application used to create, receive, retain and transmit messages and other records. Excluded from this definition are file transfer utilities.
(4) Electronic mail transmission data-Information in electronic mail systems regarding the identities of sender and addressee(s), and the date and time messages were sent.
(5) Electronic media-All media capable of being read by a computer including computer hard disks, magnetic tapes, optical disks, or similar machine-readable media.

(6) Electronic record-The information that is maintained in electronic format in a computer for computer processing and the product of computer processing of that information that satisfies the definition of a state record in the Government Code §441.180.
(7) Electronic records system-Any information system that produces, manipulates, and stores state records by using a computer.
(8) Mailing list service-An electronic mailing list hosting service (e.g., Listserv) used for discussions and announcements within a specified group of individuals. Subscribers to the service participate by sending information to and receiving information from the list using electronic mail messages.
(9) Records management officer-The person who administers the records management program established in each state agency under the Government Code, §441.183.
(10) State record-Any written, photographic, machine-readable, or other recorded information created or received by or on behalf of a state agency or an elected state official that documents activities in the conduct of state business or use of public resources. The term does not include:
(A) library or museum material made or acquired and maintained solely for reference or exhibition purposes;
(B) an extra copy of recorded information maintained only for reference; or
(C) a stock of publications or blank forms.

SECTION 6. SCOPE.
This policy applies to any electronic mail messages created, received, retained, used, or disposed of using the [Water Valley ISD's] electronic mail system.

SECTION 7. RETENTION REQUIREMENTS.
The [Water Valley ISD's] approved retention schedule lists the record series that are created and the retention period for each series. It is the content and function of an e-mail message that determines the retention period for that message. All e-mail sent or received by an agency is considered a state record. Therefore, all e-mail messages must be retained or disposed of according to the agency's retention schedule. E-mail systems must meet the retention requirements found in TAC 6.94(e). E-mail generally (but not always, see the Texas State Records Retention Schedule for more information) falls into several common record series categories. These are:
(1) Administrative Correspondence, 1.1.007 - Incoming/outgoing and internal correspondence, in any format, pertaining to the formulation, planning, implementation, interpretation, modification, or redefinition of the programs, services, or projects of an agency and the administrative regulations, policies and procedures that govern them. Subject to Archival review. **Retention: 3 years**.

(2) General Correspondence, 1.1.008 - Non-administrative incoming/outgoing and internal correspondence, in any media, pertaining to or arising from the routine operations of the policies, programs, services, or projects of an agency. **Retention: 1 year**.
(3) Transitory Information, 1.1.057 - Records of temporary usefulness that are not an integral part of a records series of an agency, that are not regularly filed within an agency's recordkeeping system, and that are required only for a limited period of time for the completion of an action by an official or employee of the agency or in the preparation of an on-going records series. Transitory records are not essential to the fulfillment of statutory obligations or to the documentation of agency functions. Examples of transitory information are routine messages (can be recorded on any medium, such as hard copy message slips or in an electronic format on e-mail and voice mail); internal meeting notices; routing slips; incoming letters or memoranda of transmittal that add nothing of substance to enclosures; and similar routine information used for communication, but not for the documentation, of a specific agency transaction. Retention: AC (after purpose of record has been fulfilled).

SECTION 8. USER RESPONSIBILITIES.
It is the responsibility of the user of the e-mail system, with guidance and training from the Records Management Officer, **to manage e-mail messages according to the agency's retention schedule.** It is the responsibility of the sender of e-mail messages within the agency's e-mail system and recipients of messages from outside the agency to retain the messages for the approved retention period. Names of sender, recipient, date/time of the message, as well as any attachments must be retained with the message. Except for listserv mailing services, distribution lists must be able to identify the sender and recipient of the message. User responsibilities may be mitigated by the use of a server level automated classification system.

SECTION 9. MAINTENANCE OF ELECTRONIC MAIL.
Records created using an e-mail system may be saved for their approved retention period by one of the following:
(1) Print message and file in appropriate hard copy file.
(2) Place in InBox folders and save on personal network drive or C:drive.
(3) Save to removable disk. 3.5" disks are not recommended for retention periods of more than one year due to the instability of this medium.
(4) Transfer to an automated records management software application.
(5) Managed at the server by an automated classification system.

Note: Agency may include specific instructions for saving e-mail messages to a hard drive. For example using Microsoft Outlook E-mail Application:

1. *You can add subfolders to your Inbox. If you file your e-mail here it avoids server problems and gives you some more leeway in storing your files.*

SECTION 10. DISPOSITION OF ELECTRONIC MAIL.
The process for the legal disposition of state records (including electronic mail) is subject to the same documentation requirements as any other format or medium. This usually requires agency permission and some type of disposition log to adequately document disposition and destruction of electronic records. Section 6.95 of the Electronic Records Standards and Procedures (relating to the Final Disposition of Electronic State Records) states that:
.(b) An electronic state record that is an archival record must be maintained by the agency through hardware and software migrations and upgrades as authentic evidence of the state's business in accessible and searchable form, except as otherwise determined by the state archivist.
(d) A state agency must establish and implement procedures that address the disposition of an electronic mail record by staff in accordance with its approved records retention schedule and, specifically, must establish guidelines to enable staff to determine if an electronic mail record falls under transitory information (records series item number 1.1.057) on the agency's approved records retention schedule in order to encourage its prompt disposal after the purpose of the record has been fulfilled.

SECTION 11. USER ID TERMINATION.

All user ID's will be revoked immediately upon a user's termination of employment with the district or upon the termination of whatever status gave the user access to the E-mail system. Within three months, the data associated with that user will be deleted including all files, records, notes, unopened mail, etc.

Requesting access to the former employee's stored E-mail to review for required retention of any official record material. Upon the termination of the user's relationship with the district, the user should no longer attempt to access the system.

Acceptable Use Policy
Section II
Agreement

EMPLOYEE AGREEMENT

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 _____

Home address _____

Date _____ Home phone number _____