

ELECTRONIC COMMUNICATIONS (E-MAIL), NETWORK RESOURCES AND INTERNET ACCEPTABLE USE AGREEMENT FOR EMPLOYEES

This Electronic Communications (E-mail), Network Resources and Internet Acceptable Use Agreement for Employees (the "Agreement") applies to all Wichita Falls Independent School District ("WFISD" or the "District") employees and extends to others offered access to WFISD resources. Please read this document carefully before agreeing to participate in the District's electronic communications system. Terms and conditions set forth in this Agreement and in Board of Trustees Policy CQ are expected to be followed. Policy CQ is available from the principal and online at www.wfisd.net (see "Policy Online").

General Principles

Access to INTERNET and E-Mail is a privilege, not a right, provided to promote educational excellence in schools by facilitating resource sharing, innovation, expanding computer skills/technology, research, and communication. The Network, Internet and E-Mail are to be used in a manner consistent with the District's standards of conduct and as part of the normal execution of an employee's job responsibilities.

With access to computers and people all over the world also comes the availability of material not considered of educational value or appropriate for the school setting. WFISD firmly believes the value of educational and business resources available on the world-wide web far outweigh the potential risk of users accessing material not consistent with the District's educational goals. WFISD has taken strict precautions to deny access to these controversial materials. However, on a global network it is impossible to control all materials and an industrious user may still find a way to access them. Within reason, freedom of speech and access to information will be honored; however, access to certain content may require approval from the Superintendent and Chief Information Officer or designated representative. During the school day, teachers will guide students toward appropriate materials and resources as would families at home (information sources such as television, computers, Internet, telephones, movies, magazines, radio and other potentially offensive media). In addition, the smooth operation of the network relies upon the proper conduct of the end users who must adhere to the strict guidelines. These guidelines are provided to make the employee aware of his/her privileges and responsibilities and to ensure efficient, ethical and legal utilization of network resources. If the employee or anyone he/she allows to access their account (in breach of Section 4 of this Agreement) violates this Agreement, the employee's access will be denied or withdrawn. In addition, the employee may be subject to disciplinary action up to and including termination.

GUIDELINES

1. Personal Responsibility

By accepting an account password and related information, and accessing the District's Local Area Network, Electronic Communications and Internet System, the employee agrees to adhere to this Agreement. The employee must also agree to report any Resource or Internet misuse to the Chief Information Officer. Misuse includes violations that harm another person or another individual's property. WFISD makes no warranties of any kind, whether expressed or implied, for the service it is providing. WFISD will not be responsible for any damages suffered. This includes loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions caused by its own negligence or employee errors or omissions. Use of information obtained via the Internet is at the employee's own risk. WFISD specifically denies any responsibility for the accuracy or quality of information obtained through its services.

2. Term of Permitted Use

Network and Internet access extends throughout the term of employment provided this Agreement is not violated. This Agreement is subject to review and/or revision in June of each year. Any changes to this Agreement do not require a new agreement to be signed; however the employee is responsible for reviewing

policies annually. Note: The District may suspend access at any time for failure to sign the Agreement, technical reasons, policy violations, or other concerns.

3. Acceptable Use

Employees using the Internet are representing WFISD. Employees are responsible for ensuring that the Internet is used in an effective, ethical, and lawful manner. Examples of acceptable use are:

- Using Web browsers to obtain information in support of education and research consistent with the educational objectives of the District.
- Accessing databases for information as needed.
- Create files related to the user's job duties or professional development/school studies and store on:
 - ❖ Computer hard drive (only if necessary)
 - ❖ Network (preferred)
 - ❖ Floppy/CD

4. Unacceptable Use

Employees must not use the Internet for purposes that are illegal, unethical, harmful to WFISD, or nonproductive. Examples of unacceptable use are:

- Conducting a personal business using WFISD resources.
- Using, transmitting, receiving, or seeking inappropriate, offensive, vulgar, suggestive, obscene, abusive, harassing, belligerent, threatening, defamatory (harming another person's reputation by lies), or misleading language or materials.
- Revealing personal information, such as the home address, telephone number, or Social Security number of another person.
- Making ethnic, sexual-preference, or gender-related slurs or jokes.
- Engaging in illegal activities, violating the Employee Handbook, or encouraging others to do so.
Examples:
 - ❖ Selling or providing substances prohibited by the District's employment policy or the Employee Handbook.
 - ❖ Accessing, transmitting, receiving, or seeking unauthorized, confidential information about students, their families, or colleagues.
 - ❖ Conducting unauthorized business.
 - ❖ Viewing, transmitting, downloading, or searching for obscene, pornographic, or illegal materials.
 - ❖ Accessing others' folders, files, work, networks, or computers.
 - ❖ Intercepting communications intended for others.
 - ❖ Downloading or transmitting any District confidential information except in the performance of duties.
- Causing harm or damaging other's property. Examples:
 - ❖ Using another employee's password to trick recipients into believing someone other than you is communicating or accessing the Network or Internet.
 - ❖ Uploading a virus, harmful component, or corrupted data.
 - ❖ Vandalizing the Network.
 - ❖ Using/downloading software that is not licensed nor approved by the District.
- Jeopardizing the security of access, the Network, or other Internet Networks by disclosing or sharing password and/or impersonating others.
- Accessing, attempting to access, or encouraging others to access controversial offensive materials exposing employees to illegal, defamatory, inaccurate, misleading, infringing, or offensive materials. Everyone must avoid these sites. If you know of employees/students who are visiting offensive or harmful sites, report that use to the Chief Information Officer.
- Wasting computer resources (i.e. printer, toner, or paper) including disk space with personal documents, and pictures not related to work or school subjects. You are permitted to save some personal documents on the computer's hard drive; however they must not be created during normal work hours, interfere with the function of the computer/network, or contain otherwise controversial materials. *Caution:* Employee's rights to privacy will be respected; however, the District will not be

responsible for lost or “stolen” files. Also, when warranted, these documents become property of the District and may be subpoenaed in a court of law.

- Downloading or transmitting copyrighted materials without permission from the copyright holder. Even when materials on the Network or the Internet are not marked with the copyright symbol, ©, employees should assume all materials are protected under copyright laws—unless explicit permission to use the materials is granted. Violations of copyright law that are committed “willfully and for purposes of commercial advantage or private financial gain may be subject to criminal penalties.

5. Netiquette Rules

- Employees must adhere to the rules of Network etiquette, or Netiquette. In other words, employees must be polite, adhere to the District’s electronic writing and content guidelines, and use the Network and Internet appropriately and legally.
- The District will determine what materials, files, information, software, communications, and other content and activity are permitted or prohibited, as outlined above in item 4.

6. Employee Responsibilities

- Ensure that all communications are for professional reasons and that they do not interfere with productivity.
- Be responsible for the content of all text, audio, or images that the employee places or sends over the Network or Internet. All communications should have the employee’s name attached.
- Not transmit copyrighted materials without permission.
- Know and abide by all applicable District policies dealing with security and confidentiality of District records.
- Manually run a virus scan on any executable file(s) received through the internet if not automated.
- Avoid transmission of nonpublic student/family information. If it is necessary to transmit nonpublic information, employees are required to take steps reasonably intended to ensure that information is delivered to the proper person who is authorized to receive such information for a legitimate use.
- Teachers must diligently monitor student behavior/activities while utilizing computer resources and accessing information from the Internet. **Teachers are not permitted to share any resource password not expressly provided for student use.** *Failure to adhere to these responsibilities may expose the teacher to disciplinary actions (revoked privileges) or legal involvement (prosecution) depending on the severity of the students’ misconduct.*
- Students are permitted to carry portable drives to store and transport their work to/from school. However, Teachers are expected to scan these drives for any executable (.EXE) files and remove them. Reason: There is software available (IE UltraSurf) that can be run from a flash drive with the sole purpose of circumventing any firewalls to access District-restricted sites.

7. E-mail

The District allows e-mail access primarily for business purposes; e-mail is currently not available to students. Employees may use the District’s e-mail system for personal use in accordance with this Agreement. Employee’s personal use of e-mail is limited to lunch breaks, work breaks, and other non-working hours only. Employees may not use e-mail for personal purposes during otherwise productive business hours. Employees are prohibited at all times from using email to:

- Operate a business, solicit money for personal gain, campaign for political causes or candidates, or promote or solicit funds for an organization, religious or other personal cause not affiliated with the District.
- Advertise/post garage sales, houses, cars, or other personal property for sale to the entire District. *Exception:* Information may be briefly mentioned in a personal e-mail with less than 5 persons during non-working hours as long as Network/Internet systems are not compromised and the intended receiver does not object.
- Send, solicit, print, copy, or reply to text or images that disparage others based on their race, religion, color, sex, sexual orientation, national origin, veteran status, disability, ancestry, or age; or those containing foul, obscene, off-color, or adult-oriented language.
- Send, solicit, print, copy, or reply to jokes (text or images) based on sex, sexual orientation, race, age, religion, national origin, veteran status, ancestry, or disability.

- Spread gossip, rumors, and innuendos about employees, clients, suppliers, or other outside parties.
- Send, solicit, print, copy, or reply to messages or images that are intended to alarm others, embarrass the District, negatively impact employee productivity, or harm employee morale.
- Send electronic chain letters.
- Send e-mail copies to nonessential readers.
- Send e-mail to group lists unless it is appropriate for everyone on a list to receive the e-mail.
- Send District-wide e-mails without the supervisor's/administrator's permission.
- Subscribe to any electronic newsletters, magazines, or other electronic materials not otherwise associated to currently assigned duties.
- Download and use personal consumer-grade instant messaging (IM) software (AOL Instant Messenger, Yahoo, MSN) to transmit IM via the public internet.

8. Monitoring

Actions on the Network are traceable. Inappropriate actions can be discovered and traced to the user.

- Internet usage data is automatically stored and is subject to retrieval for District purposes at any time. In addition, live, random monitoring of Internet activity should be anticipated.
- All messages/files created, sent, or retrieved over the Internet/Network are the property of the District and may be regarded as public information.
- WFISD reserves the right to access the contents of any email messages/files saved/sent over its facilities if the District believes, in its sole judgment, that it has a business need to do so.
- All Internet activity and communications, including web sites, text and images, can be disclosed to law enforcement or other third parties without prior consent of the sender or the receiver. *This means don't put anything into your e-mail messages or internet message boards that you wouldn't want to see on the front page of the newspaper or be required to explain in a court of law.*

9. Computer Viruses/Spyware

Computer viruses are programs designed to make unauthorized changes to programs and data. Therefore, viruses can delay access to or cause destruction of District resources. Spyware and adware can compromise system performance and allow sensitive information to be transmitted outside the organization. It is important to know that computer viruses are much easier to prevent than to cure. Defenses against computer viruses include protection against unauthorized access to computer systems, using only trusted sources for data and programs, and maintaining virus-scanning software.

Spyware installation programs can launch even when users are performing legitimate operations, such as accessing Internet sites or reading e-mail. Spyware programs are designed to collect any information from your computer (including personal) and report the data back to an unidentified party. While performing this function, other systems programs may be interrupted or damaged. As a result, combating spyware requires user vigilance as well as Information Systems management and control.

- *Information Systems Responsibilities*
 - ❖ IS shall install and maintain appropriate anti-virus/-spyware software on all computers.
 - ❖ Respond to all reports of spyware installation/virus attacks, destroy any virus detected, remove spyware modules, restore system functionality, and document each incident.
- *Employee Responsibilities.* These directives apply to all employees and other authorized WFISD users.
 - ❖ Users shall not knowingly introduce a computer virus or allow spyware to be installed into WFISD computers.
 - ❖ Users shall not load any software or program files. Users shall not knowingly install themselves any anti-spyware software. Some anti-virus/-spyware software programs function as a Trojan Horse, causing up to three times more problems than they are intended to prevent. For this reason, installation will be performed by Tech Support personnel ONLY.
 - ❖ Incoming media shall be scanned for viruses before they are read. Media is defined as but not limited to: USB Flash drives, CD, DVD, Zip files, External Hard Drives, or downloaded files.
 - ❖ Users shall perform anti-spyware updates and run anti-spyware programs regularly, as directed by the Information Systems Department.

- ❖ Any user who suspects that his/her workstation has been infected by a virus shall IMMEDIATELY STOP ALL WORK at the workstation, post a notice of the event to the workstation, and call the Helpdesk.

10. Physical Security

It is District policy to protect computer hardware, software, data, and documentation from misuse, theft, unauthorized access, and environmental hazards.

- *Employee Responsibilities*
 - ❖ Portable storage devices should be stored out of sight when not in use. If they contain highly sensitive or confidential data, they must be locked up.
 - ❖ Media must be kept away from environmental hazards such as heat, direct sunlight, and magnetic fields.
 - ❖ All educational software (Edu-tainment, curriculum assistive programs, etc) will be installed by a Tech Support representative and inventoried in the campus library or the Tech Support storage facility as appropriate.
 - ❖ All textbook software (student and teacher resource media) will be installed by a Tech Support Technician and inventoried according to campus library policy.
 - ❖ Personal software installed on District computers become the property of the District.
 - ❖ Critical computer equipment, i.e. file servers, must be protected by an uninterruptible power supply (UPS). Other computer equipment should be protected by a surge protector.
 - ❖ Environmental hazards to hardware such a food, smoke, liquids, high or low humidity, and extreme heat or cold should be avoided.
 - ❖ Since the CIO is responsible for all equipment installations, disconnections, modifications, and relocations, employees are not to perform these activities. This does not apply to temporary moves of portable computers for which an initial connection has been set up by Tech Support.
 - ❖ Employees shall not remove shared portable equipment such as laptop computers from District premises without the informed consent of their administrator or supervisor. Informed consent means that the supervisor knows what equipment is leaving, what data is on it, for what purpose it will be used, and all appropriate forms have been completed/signed.
 - ❖ Employees should exercise care to safeguard the valuable electronic equipment assigned to them. Employees who neglect this duty may be accountable for any loss or damage that may result.
 - ❖ Although not a requirement at this time, employees are encouraged to secure personal insurance to cover damages of District provided laptops and equipment when signed out for use at home or abroad. This insurance covers any damages during the period the equipment is off campus and relieves the employee of any out-of-pocket expenses for repairs.

WICHITA FALLS ISD ELECTRONIC COMMUNICATION, NETWORK RESOURCES, AND INTERNET ACCEPTABLE USE AGREEMENT FOR EMPLOYEES

ALL EMPLOYEES:

I have read and understand the Electronic Communication, Network Resources and Internet Acceptable Use Agreement for Employees (“Agreement”) and agree to follow the provisions as explicitly described. I have attended training or have had this Agreement thoroughly explained to me by a Campus Technology Trainer, Information Systems representative, or Human Resources Representative. I understand that usage of the communication systems is a privilege, not a right and that failure to abide by this Agreement may result in disciplinary action from revoked access up to termination. 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 WFISD, 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. I understand this Agreement is available at www.wfisd.net and its terms may be revised annually without my written acknowledgement.

Employee’s Signature: _____ Date: _____

Printed First, Full Middle, and Last Name: _____ **ID #:** _____

School or Building: _____ Job Assignment: _____

ADDITIONAL STATEMENT FOR TEACHERS:

In addition to the statement above, I further acknowledge that it is my responsibility to monitor student behavior/actions while utilizing District computers when under my direct supervision. Any student may use the Network for individual work or in the context of another class, and I may be held accountable for a student’s misuse of the network only while under my observation. I am aware of the requirement to scan student flash drives for .EXE files and remove them prior to their use on District computers. I fully understand the risks of sharing my password (and that sharing such password is in violation of this Agreement) and that I am responsible for any students’ malicious or inappropriate behavior while using it. As the sponsoring teacher, I do agree to instruct the student on acceptable use of the Network and proper network etiquette.

Employee’s Signature: _____ Date: _____

EMPLOYEE-RETURN THE SIGNED ACKNOWLEDGEMENT(S) TO THE PRINCIPAL/SUPERVISOR OR CAMPUS TECHNOLOGY TRAINER (CTT). PRINCIPAL/SUPERVISOR OR CTT-MAKE ONE COPY FOR THE EMPLOYEE AND SEND THE ORIGINAL SIGNED DOCUMENT(LAST PAGE) TO INFORMATION SYSTEMS.

This space reserved for systems administrators.

Assigned User Name: _____

Assigned Temporary Password: _____

Training was completed on: _____ By: _____