Technology Handbook for Employees

Troup ISD

Table of Contents

Troup ISD
Acceptable Use Policy for Employees

The Purpose of the Acceptable Use Policy (AUP)

The Purpose of the Troup ISD Acceptable Use Policy for Employees is to educate; to provide protection against violations of privacy; to prevent misuse of public resources; to protect against inappropriate or destructive behaviors which occur as a result of access to electronic information resources; and, **to ensure that technology resources provided through TISD are dedicated to improving student achievement and school administration**. The AUP also defines school district parameters for acceptable use and specify the disciplinary measures to which those who violate the policy are subject.

Child Internet Protection Act (CIPA) (Pub. L. 106-554)

The Children's Internet Protection Act (CIPA) is a federal law enacted by Congress to address concerns about access to offensive content over the Internet on school and library computers. Troup ISD subscribes to Internet services through SuperNet II. In accordance with CIPA, Troup ISD utilizes filtering & firewall tools in an effort to block objectionable materials from user access. Filtering software is not 100% effective; while filters make it more difficult for objectionable material to be received or accessed, filters are not a solution in themselves.

Internet Safety Policy For Troup ISD in Compliance with FCC-11-125A1

It is the Policy of Troup Independent School District to:

- prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications;
- prevent unauthorized access and other unlawful online activity;
- prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and
- comply with the Children's Internet Protection Act [Pub. L. No. 106-554 and 47 USC 254(h)].

Definitions

Key terms are as defined in the Children's Internet Protection Act (CIPA)*

- Access to Inappropriate Material: To the extent practical, technology protection measures (or "Internet filters") will be used to block or filter the Internet, or other forms of electronic communications, and access to inappropriate material/information.
- As required by CIPA, blocking will be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors.
- Subject to staff supervision, technology protection measures may be disabled or, in the case of minors, minimized only for bona fide research or other lawful purposes.

Inappropriate Network Usage

To the extent practical, steps will be taken to promote the safety and security of users of the Troup ISD online computer network when using electronic mail and other forms of direct electronic communications.

As required by CIPA, prevention of inappropriate network usage includes:

- unauthorized access, including so-called "hacking", and other unlawful activities; and
- unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

Education, Supervision, and Monitoring

It will be the responsibility of all members of the Troup Independent School District faculty and staff to model, educate, supervise, and monitor appropriate usage of the online computer network and access to the Internet in accordance with these policies, CIPA, the Neighborhood Children's Internet Protection Act, and the Protecting Children in the 21st Century Act. Training will include a focus on the education of students regarding appropriate online behavior including interacting with other individuals on social networking websites and in chat rooms, and regarding cyber bullying awareness and response.
Procedures for the disabling or otherwise modifying any technology protection measures will be the responsibility of the technology director of Troup ISD and/or the network manager of Troup ISD.

Troup ISD Electronic Communications Systems
The use of network and electronic resources is a privilege, not a right. Inappropriate use may result in the cancellation of the privilege. Certain state and federal statutes may apply to the electronic communications system and inappropriate uses may also be unlawful. Unlawful use of district electronic resources will be referred to proper authorities. District authorities, under the rules of the Employee Handbook, may also initiate other disciplinary actions.

Should a district user violate any of these provisions listed here, his or her account may be terminated, future access may be denied and disciplinary actions taken under the guidelines of the Employee Handbook. In addition, all users are held responsible for understanding that the inappropriate use of the communication system may be a violation of state, federal, and local laws, including but not limited to: Section 1030 of Title 18 of the United States Code Fraud and Related Activity in Connection With Computers, as well as the Texas Computer Crimes Statute, Section1, Chapter 33.02 of Title VII of the Texas Penal Code, Breach of Computer Security, and Section 16.04 of Title IV of the Texas Penal Code Unlawful Access of Stored Communications. Violations can lead to investigation and prosecution by law enforcement agencies.

Each user must attend training on appropriate use and Internet access, as well as sign a form acknowledging the rights and responsibilities of access to the electronic communications system. In those cases in which the user is under 18 years of age, the parent or legal guardian will be required to read the appropriate technology policies and to sign a form affirming that he/she has read and understands the policy and rules. ***No employee account will be granted until the employee has been through training/orientation and has signed the required forms. No student account will be opened until the student and parent (when appropriate) have signed the required forms.*** Parents may sign a form explicitly exempting their minor children from Internet access.

Usernames, email addresses, and network account names will not be changed unless the user legally changes his or her name. The user must then notify the business office as deemed appropriate. The business manager will subsequently notify the technology department that an official name change has been requested and authorized.

No student will be required to use the Internet to complete assignments when the parent denies access.

Personal information such as home address, home telephone number, or addresses and phone numbers of any other individuals should not be revealed. A personal signature on any Internet message must use the school address only. Always notify the network administrator immediately if any individual is encouraging actions that may be wrong or illegal.

The district's system is provided on an as is, as available basis. The district does not make any warranties, whether expressed 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 the functions or services performed by, or the information or software contained on, the system will meet the system user's requirements, or 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 provider and not the district. *The user is responsible and liable for any misuse of the system or system resources.* The district will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the district's electronic equipment.

The district will provide training in the use of network resources. All users can download a copy of the ***Troup ISD Technology Handbook*** at www.troupisd.org. All training in the use of the district's system will emphasize the ethical use of technology resources.

Employees supervising students who use the district system will provide training emphasizing the appropriate use of this resource to those students. <u>Students must be supervised while using district computers and/or the Internet.</u>

Best Practices for Appropriate use of Technology

The term "Best Practices" details at a minimum what employees and students should and should not do as well as the guidance of Digital Citizenship. Generally, employees and students think of best practices only in the sense of email and internet use. This AUP also extends to: computer hardware and peripherals; software; network access; storage devices: databases, files, and other repositories of information in electronic form. Best practice applies to use while onsite and when using remote access or district equipment from any remote location such as home, conference locations, or any other location other than the TISD facilities.

Availability of Access

Access to the district's electronic communications system, including the Internet, shall be made available to students, employees, and the community primarily for instructional and administrative purposes and in accordance with administrative regulations. **Limited personal use of the system is permitted if the use**:

1. Imposes no tangible cost on the district; and
2. Does not unduly burden the district's computer or network resources; and
3. Has no adverse effect on an employee's job performance or on a student's academic performance; and
4. Does not interfere with the work of other district employees; and
5. Is not utilized for personal shopping, product advertisement, including personal property, merchandise, and management of personal finances including stocks/bond, credit cards, or bank accounts.
6. Is not used to defame Troup ISD or other employees of Troup ISD.
7. Political lobbying is also prohibited.

E-mail Use —Responsible Use

The district currently utilizes Outlook Web Access (OWA) for e-mail. The following rules are representative (but not inclusive) of how the email is to be used as determined by the district.

Note that electronic mail (e-mail) is not guaranteed to be private. District officials who operate the system do have access to all e-mail. Errors may occur that miss-route mail to accounts other than those to which it is originally addressed. In addition to this, TISD faculty and staff should be aware that all e-mail is subject to open records requests in accordance with the Public Information Act (a.k.a. Texas Open Records Act.) Monitoring of e-mail by designated staff may occur on occasion to ensure appropriate use. **Messages relating to or in support of illegal activities will be reported to the authorities *(school, local, state, or federal).***

- Not everyone is eligible for an e-mail account. Student e-mail accounts will be assigned on an as needed basis for the sole purpose of completing assignments as required by the classroom teacher. The use of a student e-mail account must be in support of education and/or research as well as remain consistent with the educational objectives of the district.

- For security purposes, employees may not establish nor access personal e-mail accounts such as G-mail, Hot-mail, Yahoo Mail, AOL, Juno, or other mail service providers while at school.
- Due to network security, new employee network and e-mail accounts will not be issued until the following conditions are met: 1) the school board has approved the individual for employment; 2) official contract term has begun; 3) the new employee has participated in training and orientation for appropriate use of network resources; 4) the new employee has read and signed a user agreement and it is on file with the technology director. Email accounts will be deactivated when the individual is no longer employeed by the district.
- Use of district email for commercial activities is prohibited (i.e. contests, stock trading, etc…).
- Use of district email to purchase and/or sell products is not permitted.
- Use of district email for product advertisement, including personal property, or political lobbying is prohibited.
- Sending of Chain Letters or broadcast messages (spamming) to lists or individuals, and any other types of use, which may cause congestion of the networks or otherwise interfere with the work of others is prohibited. This includes forwarding junk mail to other users.
- Transmission of information, which violates or infringes on the rights of any person, including students, or any abusive, profane, or sexually offensive information is prohibited.
- In order to conserve system resources, technology staff will conduct clean up of district systems at least once per school year. Clean up may include removal of all e-mail, documents, etc..on electronic devices.
- Employees should never attempt to access another teacher's e-mail account.
- Employees should never use the district email system to violate the confidentiality of other employees or students.

Netiquette (Network Etiquette)

Netiquette is a term describing the generally accepted rules of behavior on networked systems. District staff and students are expected to abide by these rules and access will be revoked for violations as deemed appropriate by district administrators.

- Use appropriate language. Do not swear, use vulgarities, or any other inappropriate language.
- Illegal activities are strictly prohibited.
  Do not reveal the personal addresses, phone numbers, or other pertinent information of any students or district employees
- Minimize spelling errors. Be sure the message is easy to understand and read.
- Use accurate and descriptive titles for messages and articles. Tell people what it is about before they read it.
- Get the most appropriate audience for the message, not the widest.
- Remember humor and satire are very often misinterpreted.
- Forgive the spelling and grammar errors of others.
- Remember all network users are human beings.
- Do not perform unauthorized technical support (work) on district equipment.
- Do not use the network in such a way as to disrupt the use of the network by other users.

Security

Security on any computer system is a high priority, especially when the system involves many users. If a security problem on the District network can be identified, notify a building or system administrator. **Do not demonstrate the problem to other users.**

Passwords: Passwords are an important part of your network access. You should not use the same password for every application. In some cases, you may be required to change your password to certain applications on a regular basis. In all cases, passwords should generally be 6 or more characters in length and should contain letters, numbers, and symbols (!,*, ~, $, etc...). Passwords should be memorized and not written down and stored in a location accessible to others.

Using another individual's account and password is prohibited. A network user who allows another individual to use his/her network account may lose network privileges. **Each employee is responsible for the protection**

of his/her account password. Account names and passwords should not be shared with other individuals, particularly non-district employees. If an individual is suspected of using another's account, notify the system administrator immediately.

Attempts to logon to the network or network resources as a system administrator or to perform system administration tasks may result in cancellation of user privileges. Any user who is a security risk or having a history of security problems with other computer systems may be denied access to district network resources.

Anyone illegally obtaining and using access to other computer systems may be the focus of state or federal investigation and prosecution. Applicable state statutes include Section 16.04, Unlawful Access to Stored Communications, and Section 33.03, Breach of Computer Security.

If unacceptable or illegal activities take place while a user account is active, the account owner may be held responsible, regardless of whether that owner personally took the actions. Such activities may result in loss of access to computers and the Internet or other disciplinary actions.

Anyone knowingly having, transporting or distributing any computer virus will immediately lose access to the Internet and all district computer resources.

Guidelines for Safe Use of Computer Resources

The possibility of encountering objectionable material does exists and the district is unable to completely prevent access to such material. Efforts are made on a regular basis to block such objectionable sites. **However, if a user accesses a site with information that contains objectionable material, he or she is to exit from the site immediately and inform a principal or tech support personnel. All Internet activity is monitored and logged by the district's filter. Administrators regularly review the logs files and user history.**

Using electronic information resources can be of great educational benefit and allow teachers and students to meet people from all over the world. People may misrepresent themselves. TISD faculty and staff will take every precaution to supervise use in order to ensure that Internet access is an appropriate and positive educational experience. However, many individuals also have internet access at home. In order to ensure safety and positive outcomes from such access, Troup ISD strongly recommends users (employees & students) follow the guidelines that are provided.

Responsible use of computing and communications facilities and services requires the user to:

- Respect the legal protection provided by copyright and license of programs and data.
- Respect the rights of others by complying with all district policies regarding intellectual property.
- Respect the rights of others by complying with all district policies regarding sexual, racial, or other forms of harassment, and by preserving the privacy of personal data.
- Respect the privacy of others by not tampering with their files, passwords, or accounts, or representing others when messaging or conferencing.
- Students and employees may be issued a laptop and will also have access to workstations in computer labs, the campus library, and in some classrooms. For security purposes and confidentiality, students are not allowed to use computers designated for district employees, including teacher computers.
- All employees should log off or lock their computer each time they walk away from it.
- Classroom computers have been placed near network drops and may not be relocated to other areas in the classroom. Computers are not to be moved or relocated to other classrooms, nor removed from computer furniture and the area to which they were assigned.
- Use only computer IDs or accounts and communications facilities authorized for teacher use and use them for the purposes for which they were intended.

- Respect the integrity of computing systems and data. For example, do not intentionally develop programs *(such as viruses)* or make use of already existing programs that harass other users. Infiltrating a computer or computing system, and/or damaging or altering the software components of a computer or computing system, or gaining unauthorized access to other facilities accessible via the network is prohibited. **Additionally, personal computers/laptops or other computing devices such as MiFi Hotspots or similar devices, tablets, iPads, etc… may not be utilized at school due to potential security issues, filtering requirements, computer viruses, and/or theft.**

Guidelines for Educators Using Social Networking Sites

(Please view District Legal Policy DH at http://www.tasb.org/policy/pol/private/212904/)

Social networks are rapidly growing in popularity and use by all ages. Most social networking sites are not specifically designed for educational use. Sites such as Facebook, MySpace, Bebo, and Xanga, along with many others, provide opportunities for staying in touch with friends and family, but may NOT be accessed during the school day or by using district resources.

Educators have a professional image to uphold. How we conduct ourselves online helps determine this image. The media has reported situations where educators have demonstrated professional misconduct while engaging in inappropriate dialogue about their schools and/or students, as well as posting pictures and videos of themselves engaged in inappropriate activities. Some educators feel that being online shields them from having their personal lives examined. Online identities too often become public and can cause serious repercussions.

The district strongly discourages teachers from accepting invitations to friend students on their personal social networking sites. “Friending” students often provides more personal information than one should share in an educational setting. It is important to maintain a professional relationship with students to avoid situations that could cause bias in the classroom or situations that could be construed as inappropriate.

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

Friends and Friending

- Do not accept students as friends on personal social networking sites. Decline any student-initiated friend requests.
- Do not initiate online 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 technology staff to identify and use a restricted, school-operated networking platform.

Personal Use of Electronic and Social Media

See Policy DH (located in the TISD Board Policy Online)
Electronic media includes all forms of social media, such as text messaging, instant messaging, electronic mail (e-mail), Web logs (blogs), electronic forums (chat rooms), video-sharing websites (e.g., YouTube), editorial comments posted on the Internet, and social network sites (e.g., Facebook, MySpace, Twitter, LinkedIn). Electronic and social media also includes all forms of telecommunication such as landlines, cell phones, and web-based applications.

As role models for the district’s students, employees are responsible for their public conduct even when they are not acting as district employees. Employees will be held to the same professional standards in their public use of electronic media as they are for any other public conduct. If an employee’s use of electronic media interferes with the employee’s ability to effectively perform his or her job responsibilities, the employee is subject to disciplinary action, up to and including termination of employment. If an employee wishes to use a social network site or similar media for personal purposes, the employee is responsible for the content on the employee's page, including content added by the employee, the employee's friends, or members of the public who can access the employee's page, and for web links on the employee's page. The employee is also responsible for maintaining privacy settings appropriate to the content.

An employee who uses electronic and/or social media for personal purposes shall observe the following:

- The employee may not set up or update the employee's personal social network page(s) using the district's computers, network, or equipment at any time. Additionally, the employee may not publish a student's photo, likeness, information, etc…to a personal site or another social media site such as FaceBook, YouTube, or others not mentioned here.
- The employee shall not use the district's logo or other copyrighted material without express, written consent.
- The employee continues to be subject to applicable state and federal laws, local policies, administrative regulations, and the Code of Ethics and Standard Practices for Texas Educators, even when communicating regarding personal and private matters, regardless of whether the employee is using private or public equipment, on or off campus. These restrictions include:
    - Confidentiality of student records. [See Policy FL]
    - Confidentiality of health or personnel information concerning colleagues, unless disclosure serves lawful professional purposes or is required by law. [See Policy DH (EXHIBIT)]
    - Confidentiality of district records, including educator evaluations and private e-mail addresses. [See Policy GBA]
    - Copyright law [See Policy EFE]
    - Prohibition against harming others by knowingly making false statements about a colleague or the school system. [See Policy DH (EXHIBIT)]

See *Use of Electronic and Social Media with Students,* below, for regulations on employee communication with students through electronic media.

Use of Electronic and Social Media with Students

See Policy DH (located in the TISD Board Policy Online)

A certified or licensed employee, or any other employee designated by the superintendent, or a campus principal, may utilize electronic communication with students who are currently enrolled in the district. The teacher or support personnel must comply with all communications regulations deemed appropriate between an educator and student. All other employees are prohibited from communicating with students in the district through electronic or social media.

An employee is not subject to these provisions to the extent the employee has a social or family relationship with a student. For example, an employee may have a relationship with a niece or nephew, a student who is the child of an adult friend, a student who is a friend of the employee's child, or a member or participant in the same civic, social, recreational, or religious organization. However, descretion should be used at all times when communicating with any child.

The following definitions apply for the use of electronic media with students:

- *Electronic media* includes all forms of social media, such as text messaging, instant messaging (IM), electronic mail (e-mail), web logs (blogs), electronic forums (chat rooms), video-sharing websites (e.g., YouTube), editorial comments posted on the Internet, and social network sites (e.g., Facebook, MySpace, Twitter, LinkedIn). *Electronic media* also includes all forms of telecommunication such as landlines, cell phones, and web-based applications.

- *Communicate* means to convey information and includes a one-way communication as well as a dialogue between two or more people. A public communication by an employee that is not targeted at students (e.g., a posting on the employee's personal social network page or a blog) is not a *communication*: however, the employee may be subject to district regulations on personal electronic communications. See *Personal Use of Electronic Media*, above. Unsolicited contact from a student through electronic means is not a *communication*.
- *Certified or licensed employee* means a person employed in a position requiring SBEC certification or a professional license, and whose job duties may require the employee to communicate electronically with students. The term includes classroom teachers, counselors, principals, librarians, paraprofessionals, nurses, educational diagnosticians, licensed therapists, and athletic trainers.

An employee who uses electronic media to communicate with students shall observe the following:

- **The administration recommends that employees utilize Remind 101 for communication with students.**
- The employee may use any form of electronic media **except** text messaging. Only a teacher, trainer, or other employee who has an extracurricular duty may use text messaging, and then only to communicate with students who participate in the extracurricular activity over which the employee has responsibility.
- 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.
- The employee is prohibited from knowingly communicating with students through a personal social network page; the employee must create a separate social network page ("professional page") for the purpose of communicating with students. The employee must enable administration and parents to access the employee's professional page.
- The employee does not have a right to privacy with respect to communications with students and parents.
- The employee continues to be subject to applicable state and federal laws, local policies, administrative regulations, and the Code of Ethics and Standard Practices for Texas Educators, including:
  - Compliance with the Public Information Act and the Family Educational Rights and Privacy Act (FERPA), including retention and confidentiality of student records. [See Policies CPC and FL]
  - Copyright law [Policy EFE]
- Prohibitions against soliciting or engaging in sexual conduct or a romantic relationship with a student. [See Policy DF]
- Upon request from administration, an employee will provide the phone number(s), social network site(s), or other information regarding the method(s) of electronic media the employee uses to communicate with any one or more currently-enrolled students.
- Upon written request from a parent or student, the employee shall discontinue communicating with the student through e-mail, text messaging, instant messaging, or any other form of one-to-one communication.

An employee may request an exception from one or more of the limitations above by submitting a written request to his or her immediate supervisor.

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. 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 policies or personnel.
- Do not post images that include students without parental consent.

Audio Visual Policy

Audio visual items such as videos, films, DVDs, and other visual recordings shall be used in the classroom for educational purposes only. No audio visual item shall be shown to a class or group of students for entertainment purposes. Each audio visual item used shall meet the following criteria.

1. Have a current, relevant, aligned, instructional objective for the specific content area in which it is used.
2. Be previewed by the teacher prior to showing.
3. Be copyright compliant. U.S. Copyright law explicitly permits the use of sound and video recording without Public Performance Rights, including those marked for "home use only" when used in an educational, not-for-profit situation.
4. The District shall own audio visual items used in the classroom unless specifically approved by the campus principal prior to showing the video. Neither students nor teachers may bring videos from home for use in the classroom without the express consent of the campus administrator.
5. Personal Netflix and other such accounts should not be used since the corporate policy of such companies restrict utilization to home use. Refer to item #3 above.
6. Substitutes and/or students are prohibited from showing videos in the absence of the teacher.
7. Student assessment shall be an integral part of the instructional use of audio visuals utilized in the classroom, i.e. testing, group discussion, lesson extensions, etc. Assessments shall take place in a timely manner.

Intellectual Property Rights

Other district personnel may utilize any computer product created by an employee, for use within in the district, during and after the term of employment for that person.

Other works created by students and district employees may not be posted or published on the districts web pages without written consent. This may include, but is not limited to letters, poems, art work, song lyrics, music, etc… All materials posted on district web pages that were created by students and district employees may not contain personal information about that person or persons. See ***Troup ISD Web Publishing Guidelines*** for further information.

Web Publishing Guidelines

The purpose of the Troup ISD web site is to promote educational excellence in Troup Schools by facilitating resource sharing, innovation, and communication. Not all of the Internet capabilities listed above will be immediately available to faculty, students, and staff via the district's Web server. The Technology Director or his/her appointee will be the designated District Webmaster. The Webmaster is responsible for maintaining the District web site.

Web contacts will be selected from each campus to assist with the creation and development of campus and organizational web pages. Web contacts will also be responsible for submitting potential web pages to the Webmaster. Not all web pages will be posted on the District's web server.

Below are guidelines that will aide in the construction of all web pages posted on the District web server. These guidelines *do not* replace the Troup ISD Acceptable Use Policy.

The personal information of students may *not* be published on the District web pages or other sites such as social media sites without a signed release form or written statement. This information includes but is not limited to names, e-mail addresses, photos, personal addresses, fax numbers, phones numbers, and personal cell numbers**.**

I. **The District has established a web site for the purpose of promoting positive information about Troup ISD. Additional pages will be made available to the following individuals and organizations:**
   - Teachers desiring to publicize their class projects and success stories
   - Organizations whose purpose is to promote organizational information and positive student outcomes
   - Students, under the direct instruction of a teacher, for the purpose of fulfilling a class assignment
   - School affiliated organizations such as the PTO, Alumni Association, and booster clubs

II. **Campus, class, and organizational web pages:**
   - Facebook and/or social networking sites are not allowed for this purpose
   - Web pages produced for campuses, classes, and organizations can present information about the specific school, class, or organization's activities and should not be published on off-site servers
   - Principals are responsible for approving the content of their school based web pages and gathering staff release forms
   - Teachers are responsible for the content of all student created web pages and for acquiring the appropriate parental/guardian signed release forms
   - Organizational sponsors are responsible for the content of their organization's web page and for acquiring the appropriate parental/guardian signed release forms for students
   - All web pages are subject to review at any given time and may be rejected and removed from the network if deemed inappropriate by the campus principal, teacher, and/or webmaster

III. **Student web pages:**
   - A release form must be signed by parent(s) and/or legal guardians
   - The form must be on file with the Technology Director and sponsoring teachers will maintain a copy for their own records
   - Students may publish web pages to a district server only in conjunction with specific class projects
   - Students must have the approval of the campus principal and follow the appropriate web publishing guidelines before posting a web page
   - All student web pages will contain the following statement: **"This is a student web page. The opinions and ideas expressed here are attributed to the student and not to Troup ISD."**
   - All web pages are subject to review at any given time and may be discarded if deemed inappropriate by the campus principal and the webmaster

IV. **Teacher and sponsor responsibilities:**
   - Teachers and sponsors are responsible for gathering signed release forms for students publishing web pages and using the Internet in conjunction with class assignments or for the promotion of an organization
   - One copy of the form is to be maintained by the teacher or sponsor and the original forms will be held on file by the Technology Director
   - Teaching HTML to students when requiring web construction as part of a class assignment
   - Requiring students to research *ALL* links to other pages and sites to ensure that linked sites are appropriate and not objectionable
   - Testing all links
   - Editing and proofing student submitted web pages
   - Approving student web pages to be placed on the District WEB server - final approval rests with the webmaster
   - Determining a time limit for the page to reside on the web server – not to exceed the length of one school year
   - Notifying the webmaster of expired web pages
   - Students, faculty, & staff are to follow copyright and permission laws when producing web pages. Appropriate language and grammar is to be used at all times.

Technology Services and Support

Faculty and staff are encouraged to contact technology support staff whenever necessary for the purpose of troubleshooting and network problem solving. Support staff members are divided into three categories: Network support, Web support, and PC Troubleshooting and Upgrades. Technology support personnel are available to assist with such needs.

Equipment Support

In order to receive technical support, faculty and staff should complete a HelpDesk request through Eduphoria. Some technical problems will take priority over others; however, every effort will be made to fulfill requests in a timely manner. **A HelpDesk request is required before work can begin on a specific problem.** Upgrades will be completed only if funds are available. **No unauthorized repairs or upgrades will be performed on district owned equipment.** Sales representatives and/or students are not allowed to perform technical work on district equipment without the approval of the technology director. HelpDesk requests will be reviewed by the technology director and assigned to the appropriate individual.

Release and Use of Technology Equipment

Most classrooms are equipped with a wide variety of technology equipment. Additional equipment is available to teachers and students for class projects. A request for such equipment should be submitted via the HelpDesk in Eduphoria. This includes but is not limited to:

Computers
LCD Projectors
VCR's
Scanners
Printers
eInstructor Clickers
Interactive Whiteboards
Laptops
Televisions
DVD Players
Digital Cameras
iPods
Speakers
Mobile Labs
Digital Video Cameras
iPads

Teachers are responsible for the use of the equipment in their classrooms. Laptop computers, digital cameras, digital video cameras, etc… will be housed in campus libraries available for checkout by teachers. Equipment will be made available on a first come, first serve basis unless other arrangements have been made with the campus librarian. All equipment is to be returned at the end of the day and may not be kept overnight unless special arrangements are made with the technology director. Teachers must check out the equipment when needed. **Equipment will not be released to students.**

Equipment/Software Purchases or Online Subscription Services

All technological equipment/software purchases must have the approval of the campus principal and the technology director. Computers and other technology equipment will be purchased through the technology director. This is simply to ensure that we maintain a consistency in purchasing and that new equipment meets the specifications as set forth in the TISD Technology Plan.

Classroom Equipment: All equipment installed in the classrooms such as Interactive whiteboards, LCD projectors, and document cameras should be considered permanent fixtures in the classroom. Equipment will not be relocated unless a structural building change takes place. While the district respects the right of the teacher to arrange seating in his/her classroom, funds, personnel, and resources are not available to rearrange installed equipment each time a teacher desires to re-organize a classroom. Additionally, computers that utilize a network drop may not be relocated unless the request is reasonable and does not require additional cabling. Due to safety restrictions as well as connectivity issues, extra-long cables cannot be added to classroom computer arrangements.

New Equipment: All technology equipment purchased for Troup ISD must have the approval of the technology director and be listed on the appropriate inventory forms. Immediately upon receipt of the equipment (in good condition), an inventory form must be submitted to the business office for processing. The form must be filled out accurately and in full. A UPC label will then be sent to the responsible person for placement on the equipment.

Old and Worn Equipment: A goal of the district technology department is to provide teachers and students with equipment that is maintained and in good condition. To meet this goal, it is sometimes necessary to retire old and worn equipment. If such equipment is encountered, submit a request for removal of the items in Eduphoria's HelpDesk. Designated staff will begin the process for removal and/or replacement whenever possible. A record of the removal of this equipment must also be made on the appropriate inventory form.

Online Subscription Services: Due to ever increasing demand on bandwidth, all online subscription services requiring audio or video streaming must be approved by the network manager or the technology director.

Electronic Gradebook and Attendance Guidelines

Log on to your computer when necessary and log off of the computer when your task is complete. Do not leave your computer logged onto the network when you are not using it. Do not share your password with anyone other than a network administrator. **Passwords should be kept confidential and should not be shared with students, substitutes, or any other person.**

Teachers are required to record grades, at minimum, on a weekly basis. Grades may be accessed by campus principals and the counselor during parent conferences and therefore must be up to date. Additionally, parents and students can access grades online. It is imperative that grades are promptly recorded in the gradebook.

The authority to change a student's grade rests solely with the teacher of the student except when a violation of the law by the teacher occurs. In such a case the campus administrator shall have authority, according to law, to mandate a change of grade.

Attendance must be taken promptly and submitted electronically within the first 15 minutes of each class. Students are not allowed to access computers designated for employee use for any reason including, but not limited to e-mail, Internet access, Accelerated Reader or other programs. Teacher computers are connected to the e-mail server, as well as the gradebook and attendance server. It is a potential breech in security and confidentiality if you allow a student to use your computer. You are in essence supplying access to critical programs and confidential information.

Substitutes will not be allowed to access computers designated for employee use. Substitutes may not access the electronic gradebook and attendance program for any reason. The campus attendance clerk will be responsible for printing a classroom roster for use by the substitute in checking attendance. Substitutes must send the attendance rosters to the office for data entry within the first 15 minutes of each class. The only exception to this is in the case of long term substitutes. In such cases, the long term sub will receive similar network access that a teacher is assigned.

Unless a substitute has received technology training and is aware of district policies regarding appropriate use of the district's network and information systems, they should not be assigned the oversight of student computer use and/or student use of a computer lab including the use of mobile computer labs.

Any employee deviating from these guidelines is subject to official reprimand and other actions as deemed necessary by district administrators.

Employee Use Agreement & Web Release Form:

Please review the release form listed below. You should note that the following release form does not replace the Troup ISD Responsible Use Policy or imply permission to use Internet services. Troup ISD may choose to publish school related information on the district's website. This may include work related e-mail addresses, photos, and information of faculty and staff such as a campus or district directory. By signing this release form you are granting permission for the district to publish your photo and district e-mail address to the district's website and that it is available to anyone via the web. You should keep a copy of this form for your records. The original form will be kept on file with the Technology Director or his/her designee.

Employee Use Agreement & Web Release Notification

Troup Independent School District

Responsible Use of the District's Electronic Communications System

The Troup Independent School District is offering access to electronic equipment, the Internet and a district-based World Wide Web server to TISD faculty, staff, and students for the purpose of pursing educational goals. Access to these resources is considered a privilege and district policies, regulations, and procedures have been developed to address the issues and concerns raised by access to electronic information. In addition to the general policies, regulations, and procedures that must be adhered to by all district personnel and students accessing the network systems, faculty and staff will have a number of additional responsibilities for maintaining adherence to policies regarding use of the Internet. Such responsibilities are in keeping with the standards and practices outlined in the Code of Ethics and Standard Practices for Texas Educators – DH(E) and policy CQ.

Employees will be responsible for attending Internet training sessions prior to teaching courses to students who will be provided Internet access as part of their course work. **Employees will be responsible for monitoring students in the use of the Internet and for distributing and collecting the student's signed consent forms.** Employees are also responsible for keeping a copy of these forms on file and forwarding the original to the technology director. Employees will be professionally responsible for closely monitoring student conduct on the Internet during class sessions and during extended activities. Employees may ask a student to print a history of sites that have been accessed during any specific Internet session to verify the educational relevance of the site. Resources should be restricted to specific class usage. Examples: Use of Internet Relay Chat sessions or access to "Usenet Groups" and games is not permitted. Employees are responsible for regulating access to the Internet and other network resources. Employees must also report any violations of Internet use and network access directly to the campus principal and technology director. The campus principal will enforce disciplinary actions. Violators will lose all computing access.

Students may be allowed to assist in the development of web pages. However, employees must preview and approve proposed content and linkages of those pages. Not all web pages designed by and for students will be posted. Personal information of any kind relating to a student is strictly prohibited without written consent. Pictures that allow a student to be identified by name are prohibited. Home pages will be posted to the district's web server only after further review by the campus principal and/or Webmaster. Only the Webmaster or his/her designee will be allowed to upload files to the district web server after the review process.

Commercial use of the Internet is not acceptable, including entering contests. Personal purchases will not be permitted using the district network resources. Student access to the Internet may be denied by parental action and the teacher cannot consider student use mandatory. Students who do not have access to the Internet must be provided with alternative means for completing class assignments. Because of limited disk space and the potential for negative impact on system performance students, staff, and faculty will not be allowed to download, store, and/or run **any** software (shareware or freeware) from the Internet (including, but not limited to, AOL Instant Messenger & Yahoo Messenger service) without permission from the network system administrator. In the case of shareware, the author expects reimbursement. Any user downloading shareware is expected to reimburse the author for the privilege of using the software. The district will not be responsible for shareware downloading or fees. Shareware may not be stored on district equipment without permission from the technology director. Unauthorized software will be removed from district computers. Employees will be responsible with following through on suspected violations of technology policies and procedures by individuals, whether during their class or not.

Faculty and staff will intervene if there is any suspected violation of policies on use of copyrighted materials. Employees who assign or even suggest Internet use for class assignments must teach and monitor proper copyrighting and appropriate referencing of materials. Teachers and district staff recognize that computer files and e-mail have the same legal status as other district communications and files that are subject to public access. Teachers and district staff recognize that illegal activities and activities that are contrary to state or federal law can result in disciplinary action or charges being brought against district personnel who are found to engage in or permit such activities using district computers and network resources. Relevant statutes are **Section 16.04 Unlawful Access to Stored Communications** and **Section 33.02 Breach of Computer Security**. Users, including faculty, staff, students, and community members may not use district electronic resources to access, acquire, and/or bring through the district's network obscene, offensive, or objectionable material. The system has been financed by public money and grants and is not intended for the private use of individual staff. Access to Internet sites can be monitored and tracked by system administrators.

Employee's Name (Please print): ____

___________________________________ ___________________________________

Employee Signature Date

Please keep a copy of this form for your files. The original form must be submitted to the campus secretary for filing with the technology director.

Troup ISD Laptop Agreement

Laptop Checkout Policy

Laptop computers at Troup ISD are the property of TISD. The intended purpose of teacher laptops is to allow for mobility within the district, assist teachers in carrying out their professional responsibilities and instructional duties, and provide opportunities for continued professional growth.

Teachers will be allowed to take laptops home as needed, but they must be checked out through the technology department or designated library. Because the primary purpose of the laptop program is instructional use, the laptop should never be loaned to another individual, nor should a student be allowed to use the teacher's laptop.

When teachers take laptops out of the school building, they are responsible for the laptop at all times. If the laptop is damaged or stolen as a result of negligence while in the personal possession of the teacher, the teacher will assume financial responsibility.

All employees who are in possession of a district owned laptop & intend to use it outside of the school building or when school is not in session must complete a checkout form.

- □ I have read & agree to abide by the Troup ISD Technology Handbook for Employees. I understand that my use of this laptop is governed by the guidelines therein, including the guidelines pertaining to the installation of unauthorized software.
- □ I will notify the TISD Technology Department if I am retiring, resigning, taking a leave of absence, or will no longer maintain employment at TISD. I will immediately return this equipment as a result of my change of status.
- □ I agree to keep the laptop locked up in a cabinet or another safe place anytime the computer is unattended.
- □ I agree that the laptop will be on campus and in use by me during all instructional days.
- □ I agree that the laptop is not to be loaned to or used by a student or any other individual.
- □ I agree to keep the laptop locked in my room as stated above or within my home premises if removed from the classroom and taken home overnight. Leaving the laptop in a locked car overnight will not be considered taking the proper steps as required.
- □ I agree to return the laptop for any and all updates at the request of the Technology Department.
- □ I agree that no unauthorized repairs or work will be done to the laptop while in my possession.

Laptop Checkout Form

Teacher's Name (please print):____

Laptop Make/Model/Serial/Barcode: ____

Checkout Date: ____________________ Checkout Reason: ________________________

Check In Date: ____________________

I have read and do accept the Troup ISD Teacher Laptop Checkout Policy. I understand that while in my possession the laptop is my sole responsibility and that I will pay for any damages that might occur during that time.

_________________________________ ________________________

Signature Date

Troup ISD
CELL PHONE USAGE AGREEMENT
(Designated Users)

For employees who are issued district cell phones: Your signature below verifies that you have read and understand the Cell Phone Policy and the guidelines, procedures and responsibilities outlined below and agree to comply with them.

Guidelines

1) All users issued a School District Cell phone must sign a District cell phone user agreement form.
2) Use of School District cell phones is for School District business only.
3) School District cell phones shall not be used for personal calls. Phone users will be held liable for non-work related calls and or texting.
6) Only cell phones and services outlined in the District cell phone contract(s) will be permitted.
8) Cell phone users are responsible for all calls and text messaging on their respective phones.

Review Procedures

Each month, cellular bills will be reviewed. A more extensive review will be conducted randomly to determine user compliance of the districts *Cell Phone Usage Agreement*. Users may also be required to reimburse the district in the event that cell privileges are being unduly abused.

User Responsibilities

1) Improper use of the cell phone can be considered misappropriation of School District funds which may result in disciplinary action.
2) A cell phone user must surrender the cell phone and accessories upon termination of employment.

Cell Phone User: ____Date: ________________

Signature of the Cell Phone User: ____________________________Date: ________________