Three Way Independent School District
Acceptable Use Policy

Three Way Independent School District makes a variety of communications and information technologies available to students and district employees through Computer/Network/Internet/Email access. These technologies, when properly used, promote educational excellence by facilitating resource sharing, innovation and communication within the district. Illegal, unethical or inappropriate use of these technologies can have dramatic consequences, harming the district, its students and its employees. Three Way ISD filters all access, however it is impossible to control all materials; therefore, the district has implemented the Acceptable Use Policy.

In accordance with the Children's Internet Protection Act, Three Way Independent School District educates staff and students regarding about appropriate online behavior, including interacting with other individuals on social networking websites (including chat rooms). Three Way ISD also educates staff and students on cyber bullying awareness to insure Internet safety, including use of email and Web 2.0 resources, and has deployed filtering technology and protection measures to restrict access to inappropriate content such as those that are illegal, harmful, or contain potentially offensive information. While every effort is made to provide the most secure and optimal learning environment by monitoring on-line activities, it is not possible to absolutely prevent access (accidental or otherwise) to inappropriate content. It is possible that you may run across areas of adult content and some material you (or your parents) might find objectionable. While the district will take reasonable steps to restrict access to such material, it is not possible to absolutely prevent such access. **It is each student's responsibility to read district policy, regulations and agreement forms and ask questions if you need help in understanding and following the guidelines for appropriate and acceptable use.**

This Acceptable Use Policy is intended to minimize the likelihood of such harm by educating district students and employees and setting standards which will serve to protect the district. The district firmly believes that the valuable information and interaction available on the computer/network/internet/email far outweighs the possibility that users may procure material that is not consistent with the district's educational goals.

Mandatory Review - To educate district employees and students on proper internet safety use and cyber bullying conduct, users are required to review these guidelines at the beginning of each school year. All district employees shall be required to acknowledge receipt and understanding of all administrative regulations governing use of the system and shall agree in writing to allow monitoring of their use and to comply with such regulations and guidelines.
The parent or legal guardian of a student user is required to acknowledge receipt and understanding of Acceptable Use Policy as part of their review of the Student Code of Conduct handbook. Employees supervising students who use the district's system must provide training emphasizing its appropriate use.

Definition of District Technology System - The district's computer systems and networks (electronic communication systems) are any configuration of hardware and software. The system includes but is not limited to the following:

- Telephones, cellular telephones and voicemail facilities;
- E-mail accounts;
- Fax machines;
- Servers;
- Computer hardware and peripherals;
- Mobile technologies;
- Software including operating system software and application software;
- Digitized information including stored text, data files, e-mail, digital images and audio files;
- Internally accessed databases or tools;

- Externally accessed databases (such as the Internet); and,
- New technologies as they become available.

Availability of Access

Acceptable Use – District electronic communication system access will be used to improve learning and teaching consistent with the district's educational goals. The district requires legal, ethical and appropriate computer/network/internet/e-mail use. The district reserves the right to monitor all technology resource activity.

Privilege - Access to the district's electronic communication systems is a privilege not a right.

Access to Computer/Network/Internet/E-mail – District's electronic communication system access is provided to all districts teachers and staff. Students may be allowed to use the local network with campus permission, but may only use the internet with parent permission. Student internet access will be under the direction and guidance of a district teacher or staff member. Access to the district's electronic communications system, including the internet and email, shall be made available to students and employees primarily for instructional and administrative purposes and in accordance with administrative regulations. Limited personal use is permitted by employees, if the use imposes no tangible cost to the district, does not unduly burden the district's computer or network resources, and has no adverse effect on an employee's job performance or on a student's academic performance. All non-employee/non-student users must obtain approval from the principal or departmental supervisor or designee to gain individual access to the district's system. All system users may not use another person's system account. Any system user identified as a security risk or having violated district's Acceptable Use Policy may be denied access to the district's system. Other consequences may also be assigned.

Subject to Monitoring - All district electronic communication system usage shall not be considered confidential and is subject to monitoring by designated staff at any time to ensure appropriate use. System users should not use the computer system to send, receive or store any information, including e-mail messages, that they consider personal or confidential and wish to keep private. All electronic files, including e-mail messages, transmitted through or stored in the computer system will be treated no differently than any other electronic file. The district reserves the right to access, review, copy, modify, delete or disclose such files for any purpose. Users should treat the computer system like a shared or common file system with the expectation that electronic files, sent, received or stored anywhere in the computer system will be available for review by any authorized representative of the district for any purpose.

User Responsibilities
System users may not use another person's system account or apply of account under false pretenses. System users may not delete, examine, copy, or modify files and/or data belonging to other users without prior consent.

Campus and Departmental-Level Responsibilities
The principal/departmental administrator or designee will:

- Be responsible for disseminating and enforcing the district's Acceptable Use Policy for the district's electronic communication systems at the campus or departmental level.
- Ensure that all individual users of the district's electronic communication systems complete and sign an agreement to abide by district policies and administrative regulations regarding such use.
- Ensure that employees supervising students who use the district's electronic communication systems provide information emphasizing its appropriate and ethical use.
- Monitor and examine all users of the district's electronic communication systems to ensure appropriate and ethical use.

Employee Responsibilities
District employees are bound by all portions of the district's electronic communication systems Acceptable Use Policy. An employee who knowingly violates any portion of the Acceptable Use Policy will be subject to disciplinary action in accordance with district policies. [See Board policy CQ Local].

Three Way ISD Employee Code of Conduct
District employees are expected to maintain appropriate conduct when accessing the communications and information technologies available through the district's electronic communication system access. All employees must comply with the district's electronic communication systems Acceptable Use Policy at all times when accessing any part of the technology system. Employees will guard and protect access to secure systems by:

1. **Protecting passwords and similar authorization information -** Passwords are the primary way in which users are authenticated and allowed to use the district's computing resources. Employees will not disclose personal password(s) to any individual, including a faculty or staff members other than the TWISD technology department. Similarly, employees will not disclose other identifying information (e.g., PIN numbers) used to access specific system information, recognizing that if they do so, they will be held accountable for their actions as well as those of other parties to whom they have given access.

2. **Guarding unauthorized use of resources -** Employees will not allow others to make use of their accounts or network access privileges to gain access to resources to which they would otherwise be denied.

3. **Not circumventing or compromising security -** Employees must not utilize any hardware or software in an attempt to compromise the security of any other system, whether internal or external to the district's electronic communication systems and network. Examples of prohibited activities include (but are not limited to) Trojan horses, password crackers, port security probes, network snoopers, IP spoofing, and intentional transmission of viruses or worms. Computer/Network/Internet/E-mail usage is subject to monitoring by designated staff at any time to ensure appropriate use. Electronic files sent, received or stored anywhere in the computer system are available for review by any authorized representative of the district for any purpose. Employees will affirm, in writing that at all times their actions while using the district's electronic communication system will not violate the law or the rules of network etiquette, will conform to the guidelines set forth in the Acceptable Use Policy, and will not violate or hamper the integrity or security of the district's technology system. If a violation of the Acceptable Use Policy occurs, employees will be subject to one or more of the following actions:

1. Revocation of access**;**
2. Disciplinary action;
3. Loss of employment with the district;
4. Appropriate legal action.

Student Responsibilities
District students are bound by all portions of the district's electronic communications system's Acceptable Use Policy. A student who knowingly violates any portion of the Acceptable Use Policy will be subject to suspension of access and/or revocation of privileges on the district's system and will be subject to disciplinary action in accordance with the Board-approved *Student Code of Conduct. [Board Policy CQ Legal]* If a student accesses an inappropriate internet file/site/email or a threatening message they must immediately minimize the program and report it to a teacher or staff member. Students must at all times use the district's electronic communication system, including email, wireless network access, and Web 2.0 tools/resources to communicate while at school, because these networks are filtered at all times. Students are responsible for backing up their own data in their network storage folder or other means such as email or the cloud. The district is not responsible for the loss of data that a student saved to these storage spaces.

Use of System Resources
System users are asked to purge e-mail or outdated files on a regular basis.

Inappropriate Use
Inappropriate use includes, but is not limited to, those uses that violate the law, that are specifically named as violations in this document, that violate the rules of network etiquette, or that hamper the integrity or security of this or any components that are connected to the district's electronic communication systems. Electronically posting messages or accessing materials that are abusive, obscene, sexually oriented, threatening, harassing, illegal, or damaging to another's reputation are prohibited. Utilizing the district's network and or equipment to cheat on assignments or tests is also prohibited. The following actions are also considered inappropriate uses and are prohibited:

Violations of Law
Transmission of any material in violation of any federal or state law is prohibited. This includes, but is not limited to:

- copyrighted material;
- plagiarized material;
- threatening, harassing, defamatory or obscene material;
- material protected by trade secret.

Tampering with or theft of components from district systems may be regarded as criminal activity under applicable state and federal laws. Using the district's electronic communication system for illegal purposes including, but not limited to cyber bullying, gambling, pornography, and computer hacking is prohibited. Any attempt to break the law through the use of a district computer/network/internet/email account may result in litigation against the offender by the proper authorities. If such an event should occur, the district will fully comply with the authorities to provide any information necessary for the litigation process.

Intellectual Property - Teachers, staff and students must always respect copyrights and trademarks of third-parties and their ownership claims in images, text, video and audio material, software, information and inventions. The copy, use, or transfer of others' materials without appropriate authorization is not allowed.

Transmitting Confidential Information - Teachers, staff and students may not redistribute or forward confidential information (i.e. educational records, directory information, personnel records, etc.) without proper authorization. Confidential information should never be transmitted, redistributed or forwarded to outside individuals who are not expressly authorized to receive the information. Revealing such personal information as home addresses or phone numbers of users or others is prohibited.

Modification of Computer - Modifying or changing computer settings and/or internal or external configurations without appropriate permission is prohibited.

Commercial Use - Use of the system for any type of income-generating activity is prohibited. Advertising the sale of products, whether commercial or personal is prohibited.

Marketing by Non-TWISD Organizations - Use of the system for promoting activities or events for individuals or organizations not directly affiliated with or sanctioned by the district is prohibited.

Vandalism/Mischief - Any malicious attempt to harm or destroy district equipment, materials or data; or the malicious attempt to harm or destroy data of another user of the district's electronic communication system, or any of the agencies or other networks to which the district has access is prohibited. Deliberate attempts to degrade or disrupt system performance are violations of district policy and administrative regulations and may constitute criminal activity under applicable state and federal laws. Such prohibited activity includes, but is not limited to, the uploading or creating of computer viruses. Vandalism as defined above is prohibited and will result in the cancellation of system use privileges. System users committing vandalism will be required to provide restitution for costs associated with system restoration and may be subject to other appropriate consequences. [See DH, FN series, and FO series in Board Policy and the Board approved *Student Code of Conduct*]

Impersonation/Plagiarism - Fraudulently altering or copying documents or files authored by another individual or assuming the identity of another individual is prohibited.

Illegally Accessing or Hacking Violations - Illegally accessing or hacking and subsequent manipulation of information of private databases/systems is prohibited.

File/Data Violations - Deleting, examining, copying, or modifying files and/or data belonging to other users, without their permission is prohibited.

Copyright Violations - Downloading or using copyrighted information without following approved district procedures is prohibited.

System Interference/Alteration - Deliberate attempts to exceed, evade or change resource quotas are prohibited. The deliberate causing of network congestion through mass consumption of system resources is prohibited. Intentionally introducing a virus or other malicious program onto the district's system or utilizing proxy gateways, or similar technologies to bypass or breach any system monitoring or filtering security measures is prohibited.

Participation in Social Media Learning Environments - Students and employees may participate in social media learning environments (such as, but not limited to, blogs, discussion forums, RSS feeds, wikis, and message boards) within a district-approved safe, secure, curriculum-supported learning opportunity. The use of these social media environments must be directly related to school assignments or class projects and not for personal use. Electronically posting personal information about one's self or others (i.e., addresses, phone numbers, etc.) is strictly prohibited.

Electronic Communication

Electronic Mail (e-mail) is one of the most used communications tools in the district. It should be us used primarily for instructional and administrative needs. All teachers, staff and students in grades 6-12 are issued email accounts and should keep the following points in mind:

- **Perceived Representation -** Using school-related email addresses might cause some recipients or other readers of the email to assume that the user's comments represent the district or school, whether or not that was the user's intention.
- **Privacy -** Email communication should not be considered a private, personal form of communication. Private information, such as home addresses or phone numbers, should not be divulged in email without the permission of the individual involved.
- **Inappropriate Language -** Using obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language in emails distributed through district email is prohibited. Sending messages that could cause danger or disruption, personal attacks, including prejudicial or discriminatory attacks are prohibited.
- **Political Lobbying -** Consistent with State ethics laws, district resources and equipment, including, but not limited to, email, must not be used to conduct any political activities, including political advertising or lobbying. This includes using district email to create, distribute, forward, or reply to messages, from either internal or external sources, which expressly or implicitly support or oppose a candidate for nomination or election to either a public office or an office of a political party or support or oppose an officeholder, a political party, or a measure (a ballot proposition). These guidelines prohibit direct communications as well as the transmission or forwarding of emails, hyperlinks, or other external references within emails regarding any political advertising.
- **Religious –** Using district email to create, distribute, forward, or reply to messages, from religious organizations or conveying a religious message to others is prohibited.

- **Forgery -** Forgery or attempted forgery of email messages is prohibited. Attempts to read, delete, copy or modify the email of other system users, deliberate interference with the ability of other system users to send/receive email, or the use of another person's user ID and/or password is prohibited.
- **Junk Mail/Chain Letters -** Generally users should refrain from forwarding emails which do not relate to the educational purposes of the district. Chain letters or other emails intended for forwarding or distributing to others is prohibited. Creating, distributing or forwarding any annoying or unnecessary message to a large number of people (spamming) is also prohibited.
- **Resource Limits -** Users should limit email messages to instructional and administrative functions. Users should check email frequently, delete unwanted messages promptly, and stay within the email server space allocations. Email attachments are limited to 2MB or smaller.

Security

Reporting Security Problem
If knowledge of inappropriate material or a security problem on the District's electronic communication system is identified; the user should immediately notify the district's technology department. The security problem should not be shared with others.

Impersonation
Attempts to log on to the District's electronic communication system impersonating a system administrator or district employee, student, or individual other than oneself, will result in revocation of the user's access to the district's electronic communication system.

Other Security Risks
Any user identified as having had access privileges revoked or denied on another computer system may be denied access to the district's computer/network/internet/email.

Consequences of Agreement Violation
Any attempt to violate the provisions of this agreement may result in revocation of the user's access to the district's electronic communication system, regardless of the success or failure of the attempt. In addition, school disciplinary action and/or appropriate legal action may be taken and possible criminal action.

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

Warning

Sites accessible via the Computer/Network/Internet/Email may contain material that is illegal, defamatory, inaccurate or controversial. Each district computer with internet access has filtering software that blocks access to visual depictions that are obscene, pornographic, inappropriate for students, or harmful to minors, as defined by the federal Children's Internet Protection Act (CIPA). The District makes every effort to limit access to objectionable material; however, controlling all such materials on the Computer/Network/Internet/E-mail is impossible, even with filtering in place. With global access to computers and people, a risk exists that students may access material that may not be of educational value in the school setting. The Three Way ISD Internet connection is the only system to be used in schools. No commercial Internet accounts may be used.

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.

Elastic Clause

The school and administration reserve the right to establish fair and reasonable rules and regulations for circumstances that may arise requiring actions that are not covered under these guidelines. In all cases, rules, regulations, and possible consequences shall be as consistent as possible with previously established rules, regulations, and consequences for similar incidents. Matters omitted from these guidelines should not be interpreted as a limitation to the scope of the District's responsibility and, therefore, the District's authority in dealing with any type of infraction that may not be in the best interest of the safety and welfare of the students. These rules and policies apply to any student who is on school property, who is in attendance at school, any school sponsored activity, or whose conduct at any time or place directly interferes with the operations, discipline, or general welfare of the District, schools, students and staff. Any system user identified as a security risk or having violated District Acceptable Use Policy may be denied access to the District's system. The use of the District's systems is a privilege, not a right and may be revoked if deemed necessary by the TWISD System Administrators. Other consequences may also be assigned. Students and Staff members of Three Way Independent School District must be in compliance with Three Way ISD Electronic Communication and Data Management Policies CQ (Local) and CQ (Legal) when using Computer/Network/Internet/E-mail access in the district.