

Acceptable Use Policy

Fabens I.S.D.

821 N.E. "G" Avenue

P.O. Box 697

Fabens, TX 79838

(915) 765-2600

Dr. Veronica Vijil, Superintendent

Fabens I.S.D. Telecommunication Network
Application for Account with Terms and Conditions for use
Revised: September 2021

CONTENTS

- I. Overview**
- II. Regulations and Guidelines**
 - A. Consent Requirements
 - B. System Access
 - C. Cybersecurity
 - D. Violations
- III. Information Content**
 - A. Internet Safety
 - B. Cyber bullying
 - C. Email Archiving and Retention
 - D. Mobile Device Responsibilities
 - E. Third-Party Supplied Information
 - F. Texas Gun Storage Safety
 - G. Disclaimer
- IV. Exhibit A – English & Spanish Letter For Parents of System User**
- V. Exhibit B – Student Agreement for Acceptable Use of the Electronic Communications System**
- VI. Exhibit C - Employee Agreement for Acceptable Use of The Electronic Communications System**
- VII. Exhibit D - Agreement for Acceptable Use of The Electronic Communications System By a Non-school User**
- VIII. Exhibit E - Parent or Guardian Release Form**
- IX. Exhibit F – Request To Unblock Web Site**

Fabens Independent School District Telecommunications Network Application for Account and Terms and Conditions for Use

I. OVERVIEW:

The Fabens ISD Network provides electronic network services and access to the students, and staff.

Our goal in providing Internet access is to promote educational excellence in the Fabens ISD and facilitate resource sharing, innovation, and communication. The Fabens ISD Network includes: Distance Learning facilities, library systems, campus systems, administrative systems, telephone systems, any other system or any other electronic telecommunication system.

Internet access is coordinated through a complex association of government, regional, and state networks. In addition, the smooth operation of the District's system/network relies upon the proper conduct of the end users who must adhere to strict guidelines. These guidelines are provided here so that you are aware of the responsibilities you are about to acquire. In general, this requires efficient, ethical, and legal utilization of the network/system resources. Use of Fabens ISD network services includes Internet access. The signature (s) at the end of this document is (are) legally binding and indicates the party (parties) who signed has (have) read the terms and conditions carefully and understand(s) their significance.

II. REGULATIONS AND GUIDELINES:

The Superintendent or designee will oversee the District's electronic communications system.

Designee is the Technology Director

The District will provide training in proper use of the system and will provide all users with copies of acceptable use guidelines. All training in the use of the District's system will emphasize the ethical use of this resource.

Filtering

The District will filter and restrict access to prohibited sites. All requests to open sites that are blocked should be requested through the campus or department administrator, including all descriptive rationale. The Director of Technology will research the sites for approval. (EXHIBIT F)

Consent Requirements

Copyrighted software or data may not be placed on any system connected to the District's system without permission from the holder of the copyright. Only the owner(s) or individual(s) the owner specifically authorizes may upload copyrighted material to the system.

No original work created by any District student or employee will be posted on a web page under the District's control unless the District has received written consent from the student (and the student's parent) or employee who created the work. [See CQ(EXHIBIT)]

No personally identifiable information about a District student will be posted on a web page under the District's control unless the District has received written consent from the student's parent. An exception may be made for “directory information” as allowed by the Family Education Records Privacy Act and District policy. [See CQ(EXHIBIT) and policies at FL]

System Access

Access to the District's electronic communications system will be governed as follows:

1. As appropriate and with the written approval of the immediate supervisor, District employees will be granted access to the District's system.
2. Students in grades (K-12) will be granted access to the District's system by their teachers, as appropriate. Students in grades (K-12) will be assigned individual accounts, which may or may not have passwords.
3. Any system user identified as a security risk or as having violated District and/or campus computer use guidelines may be denied access to the District's system.

Cybersecurity

All employees and students are obliged to protect our school data and avoid security breaches. When employees and students use their digital devices to access district emails or accounts, they introduce security risk to our data. You are advised to keep both your personal and Fabens ISD issued computer, tablet and cell phone secure. This will be done by the following:

1. Keep all devices password protected.
2. Choose and upgrade a complete antivirus software.
3. Ensure you do not leave your devices exposed or unattended.
4. Install security updates of browsers and systems monthly or as soon as updates are available.
5. Log into Fabens ISD accounts and systems through secure and private networks only.

To reduce the likelihood of security breaches, we also instruct all Fabens ISD employees and students to:

1. Turn off their screens and lock their devices when leaving their desks.
2. Report stolen or damaged equipment as soon as possible to [*HR/School Admin/ IT Department*].
3. Change all account passwords at once when a device is stolen.
4. Report a perceived threat or possible security weakness in all Fabens ISD systems.
5. Refrain from downloading suspicious, unauthorized or illegal software on their District equipment.
6. Avoid accessing suspicious websites.

We also expect all employees and students to comply with our password guidelines and email guidelines outlined in the FISD Technology Standard Operating Procedures Manual. All employees required to complete cybersecurity training annually.

VIOLATIONS

Non-severe Violations

Non-severe violations are typically those that have minimal effects on others. They include, but are not limited to:

- Using technology for off-task activities during class (games, videos, music files, CDs, web sites not instructionally related)
- Having benign executable (programs that pose no threat to network or data security) or shortcuts to them in home directory without authorization
- Using the technology for commercial purposes, online college course work, or for political lobbying.
- Accessing or attempting to access translator services, chat-rooms, bulletin boards, news groups or messaging systems other than Fabens ISD email account unless authorized by your teacher for a valid educational purpose
- Removing or replacing hardware or cables without authorization.

Severe Violations

Severe Violations are typically those that exhibit indifference to the rights of others or to one's own personal safety. *Once a student loses computer privileges due to a severe violation, any subsequent violation is considered severe regardless of the offense.* They include, but are not limited to:

- Installing unauthorized software anywhere on the network
- Downloading and storing files on the network without authorization
- Not reporting computer vandalism or network security violations that you are aware of
- Vandalizing or defacing hardware: damage less than \$50
- Using another's account or allowing another individual the use of one's account
- Using technology to cheat: to misrepresent another's work as one's own or to pass one's work on to another for the purpose of cheating
- Using technology to plagiarize or infringe copyright
- Accessing or attempting to access material that is profane, obscene, lewd, sexually suggestive or ghastly; accessing or attempting to access material that advocates or engages in illegal acts, threats, hate or violence; accessing or attempting to access material that potentially disrupts, causes damage, threatens, or endangers students or staff.
- Spamming: Distributing mass e-mail messages and chain letters or sending e-mail to large numbers of people or a large volume of messages

to one or more individuals for the purpose of causing annoyance or disruption

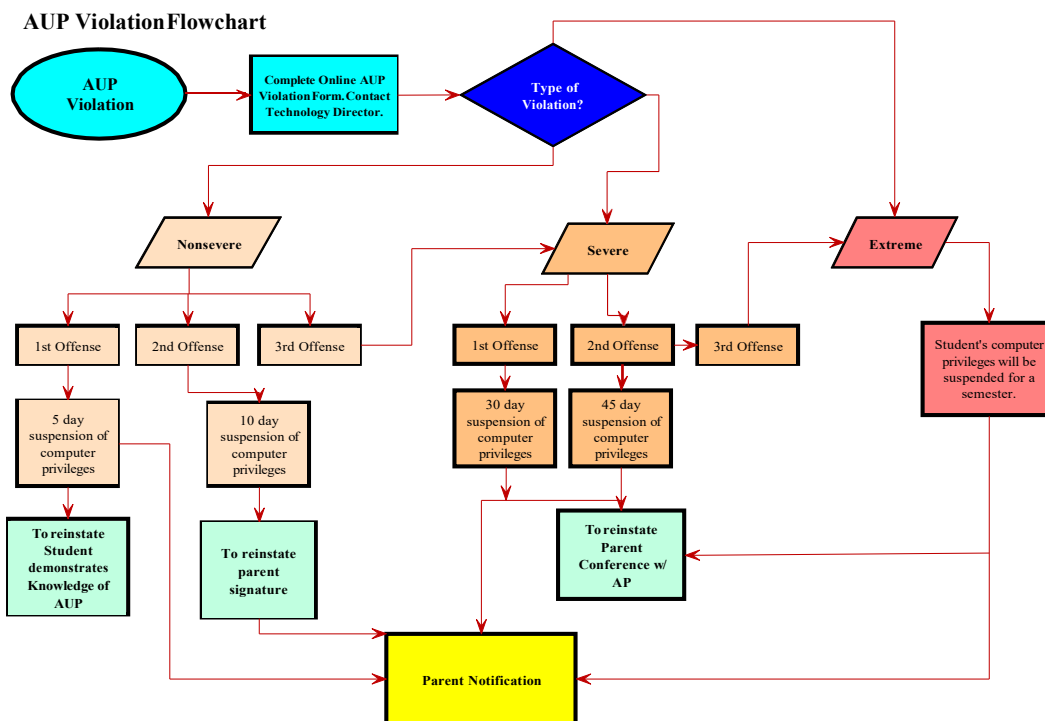
- Posting personal or private information about yourself or other people
- Posting or sending information that insults, defames or harasses

Extreme Violations

Extreme violations are acts with the potential to cause great harm to the LAN/WAN and its resources or to other people. They include but are not limited to:

- Attempting to get unauthorized access to the Fabens ISD network from any computer (including computers not at school)
- Attempting to get unauthorized access to any network from an Fabens ISD computer
- Connecting any non-Fabens ISD hardware to the network
- Cyber bullying
- Producing, posting, or sending (or attempting to do so) material that is profane, obscene, lewd, sexually suggestive or ghastly; material that advocates or engages in illegal acts, threats, hate or violence; or material that potentially disrupts, causes damage, threatens, or endangers students or staff.
- Possessing hacking tools
- Arranging a meeting with or agreeing to meet with a person you have met online
- Vandalizing or attempting to vandalize data or hardware: damage greater than \$50

X. Violation Flowchart



XI. INFORMATION CONTENT

INTERNET SAFETY

In compliance with the Children's Internet Protection Act ("CIPA"), the School District will implement filtering and/or blocking software to restrict access to Internet sites containing child pornography, obscene depictions, or other materials harmful to minors less than 18 years of age. The software will work by scanning

for objectionable words or concepts, as determined by the School District. [Note: CIPA does not enumerate any actual words or concepts that should be filtered or blocked. Thus, CIPA necessarily requires that the School District determine which words or concepts are objectionable.] However, no software is foolproof, and there is still a risk an Internet user may be exposed to a site containing such materials. An Account user who incidentally connects to such a site must immediately disconnect from the site and notify a teacher or supervisor. If an Account user sees another user is accessing inappropriate sites, he or she should notify a teacher or supervisor immediately.

In compliance with CIPA, the Fabens Independent School District and its representatives will implement a mechanism to monitor all minors' on-line activities, including website browsing, email use, chat room participation and other forms of electronic communications. Such a mechanism may lead to discovery a user has violated or may be violating this Policy, the appropriate disciplinary code or the law. Monitoring is aimed to protect minors from accessing inappropriate matter, as well as help enforce this policy, on the Internet, as determined by the school board, local educational agency or other related authority. The School District reserves the right to monitor other users' (e.g., employees, students 17 years or older) online activities, and to access review, copy, store or delete any electronic communications or files and disclose them to others as it deems necessary.

Student information shall not be posted unless it is necessary to receive information for instructional purposes, and only if the student's teacher and parent or guardian has granted permission (*EXHIBIT F*).

Account users shall not reveal on the Internet personal information about themselves or about other persons. For example, Account users should not reveal their full names, home addresses, telephone numbers, school addresses, or parents' names on the Internet.

Account users shall not meet in person anyone they have met on the Internet in a secluded place or a private setting. Account users who are under the age of 18 shall not meet in person anyone they have met on the Internet without their parent's permission.

Account users will abide by all school district security policies.

CYBERBULLYING

Fabens ISD will provide a learning environment that is free from cyber-bullying. It is a violation of this policy for any student to engage in cyber-bullying, or for any employee of Fabens ISD to condone or fail to report acts of cyber-bullying that they witness or become aware of through the use of technology or an electronic device owned, leased or used by the school district.

It is also a violation of this policy for any student to engage in cyber-bullying at a location, activity, function or program that is not school-related, or through the use of technology or an electronic device that is not owned, leased or used by the school district, if the bullying creates a hostile environment at school for the victim, infringes on the rights of the victim at school, or materially and substantially disrupts the education process or orderly operation of the school, as determined by school administrators.

Fabens ISD will not tolerate retaliation against a person who reports cyber-bullying, provides information during an investigation of cyber-bullying, or witnesses or has reliable information about cyber-bullying.

“Cyber-bullying” is defined as bullying through the use of technology or any electronic communication, which includes but is not limited to any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by such things as electronic mail, internet communications, instant message, text message or facsimile. Cyber-bullying includes (i) the creation of a web page or blog in which the creator assumes the identity of another person or (ii) the knowing impersonation of another person as the author of posted content or messages, if the creation or impersonation is a violation under the law. Cyber-bullying also includes the distribution by electronic means of a communication to more than one person or the posting of material on an electronic medium that may be accessed by one or more persons, if the distribution or posting is a violation of the law.

It is the responsibility of every student, parent and employee of the school district to recognize acts of cyber-bullying and retaliation. Any student who believes that he or she has been the victim of cyber-bullying or retaliation should report it immediately to his or her teacher or principal.

Students, parents and members of the school staff (including but not limited to

educators, administrators, school nurses, cafeteria workers, custodians, bus drivers, coaches, advisors, advisors to an extracurricular activity, or paraprofessionals), who witness or become aware of cyber-bullying or retaliation should immediately report it to the principal.

Reports of cyber-bullying will be promptly investigated. If the school principal or a designee determines that bullying or retaliation has occurred, the school principal or designee will (i) notify the police if the principal or designee believes that criminal charges may be pursued against the perpetrator; (ii) take appropriate disciplinary action; (iii) notify the parents or guardians of the perpetrator; and (iv) notify the parents or guardians of the victim, and to the extent consistent with state and federal law, notify them of the action taken to prevent any further acts of bullying or retaliation.

Any student who knowingly makes a false accusation of bullying or retaliation will be subject to disciplinary action including, but not limited to reprimand, detention, loss of privileges, and/or suspension. An educational component will be part of the actions taken. If the false accusations have civil and/or criminal elements then further actions may be taken by appropriate law enforcement agencies.

Any staff member, parent, and/or community member who knowingly engage in false accusations will be subject to appropriate consequences administered by the school system and/or law enforcement agencies.

Complaints of bullying or retaliation may be made anonymously; however, no disciplinary action shall be taken against a student, staff member, parent, or community member solely on the basis of an anonymous report.

EMAIL ARCHIVING AND RETENTION

The District email retention policy is as follows:

- All email and calendar items sent and received on the Fisd email system will be archived.
- All active employees' email will be archived for 1 year.
- Inactive employees' email will be kept in its state on the date of account disable for 6 months past their inactive date. At that time, email and email account will be fully purged from the system.
- Under request or guidance from District HR or Legal personnel, email data from inactive employees may be kept longer than 12 months.

MOBILE DEVICE RESPONSIBILITIES

Individuals who have student data on a mobile device are responsible to secure the data. It is the responsibility of the primary user of the device to immediately inform FISD Technology Department in the event of the device being lost, stolen, missing, infected with a virus/malware, hacked, or otherwise compromised. Any mobile device connected to the District network or configured to access District email is subject to FISD Tech Dept. oversight, which may include remotely erasing data on the device at any time.

THIRD-PARTY SUPPLIED INFORMATION

System users and parents of students with access to the District's system should be aware that use of the system may provide access to other electronic communications systems in the global electronic network that may contain inaccurate and/or objectionable material. A student who gains access to such material is expected to discontinue the access as quickly as possible and to report the incident to the supervising teacher.

A student knowingly bringing prohibited materials into the school's electronic environment 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 Student Code of Conduct.

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

TEXAS GUN STORAGE SAFETY

The presence of unlocked guns in homes increases the risk of both unintentional gun injuries and intentional shootings. Safe storage laws require guns to be stored locked and unloaded when any person prohibited from possessing a gun is present in the gun owner's home. Texas laws impose criminal liability on adults who negligently leave firearms accessible to children or otherwise allow children access to firearms. Practicing safe gun storage protects our kids and prevents accidents, together, we can keep our district safe.



STATE OF TEXAS LAWS PERTAINING TO SAFE GUN STORAGE AND RESPONSIBILITIES OF PARENTS/GUARDIANS

Dear Parent/Guardian:

Fabens Independent School District (FISD) is dedicated to provide a safe educational learning environment for our students and staff in all our campuses and offices.

Recently, gun violence has been on the rise at an alarming rate in schools throughout our nation. Gun violence incidents at schools have claimed the lives of many innocent children, teachers and staff. Firearms are now the leading cause of death among children in the U.S. Every year, nearly 350 children under the age of 18 unintentionally shoot themselves or someone else. Distressingly, almost 40% of child gun deaths are suicides. Studies of school-based gun violence point to these guns being obtained from the home of a parent or close relative of the student. One study found that 87% of kids know where their parents' guns are kept, and 60% have handled them.

FISD recognizes that proper gun storage education and laws are essential to ensuring a gun-free district. To further our efforts to protect students from firearms and as a courtesy to our families, Fabens ISD is informing parents and guardians of the legal obligations to protect minors from negligent gun storage. Research shows that secure firearm storage practices are associated with up to an 85% reduction in the risk of self-inflicted and unintentional firearm injuries among children and teens. Storing firearms securely protects any child in your home as well as students throughout the school district and community.

Please review the state statute on gun storage laws summarized below so that you can familiarize yourself:

Texas State Law 46.13 “Making a Firearm Accessible to a Child”

In Texas, a “child” is defined as a person under the age of 17. The statute indicates that a person commits an offense if a child gains access to a readily dischargeable firearm and the person with criminal negligence:

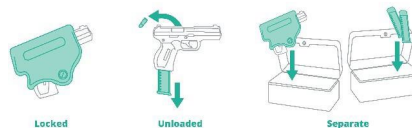
- (1) failed to secure the firearm; or
- (2) left the firearm in a place the person knew or should have known the child would gain access to.

You can learn more about gun safety, including a secure storage fact sheet, how to talk to your children about guns, obtain facts and resources at BeSMARTforKids.org.



Secure all guns in your homes and vehicles;
Model responsible behavior around guns;
Ask about unsecured guns in other homes;
Recognize the role of guns in suicide;
Tell your peers to Be SMART

Assume children and teens can find guns. Store firearms **locked, unloaded and **separate** from ammunition.**



DISCLAIMER

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 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.

See the following pages for forms that are used by the District regarding the use of its electronic communications system:

Exhibit A - English: Letter for Parents of System Users - 1 page

Exhibit A - Spanish: Letter for Parents of System Users - 1 page

Exhibit B: Student Agreement for Acceptable Use of the Electronic Communications System - 3 pages

Exhibit C: Employee Agreement for Acceptable Use of the Electronic Communications System 7 2 pages

Exhibit D: Agreement for Acceptable Use of the Electronic Communications System by a Non-school User - 2 pages

Exhibit E: Release Form for the Electronic Display of Original Work - 1 page

Exhibit F – Request To Unblock Web Site – 1 page

LETTER FOR PARENTS OF SYSTEM USERS

Dear Parents,

Your child has an opportunity to be given access to the District's electronic communications system and needs your permission to do so. Your child will be able to communicate with other schools, colleges, organizations, and individuals around the world through the Internet and other electronic information systems/networks.

The Internet is a network of networks. Through the District's electronic communications system, your child will have access to hundreds of databases, libraries, and computer services all over the world.

With this educational opportunity also comes responsibility. It is important that you and your child read the enclosed District policy, administrative regulations, and agreement form and discuss these requirements together. Inappropriate system use will result in the loss of the privilege to use this educational tool.

Please note that the Internet is an association of diverse communication and information networks. It is possible that your child may run across areas of adult content and some material you might find objectionable. While the District will take reasonable steps to preclude access to such material and does not condone such access, it is not possible for us to absolutely prevent such access.

Please return the attached agreement form indicating your permission or denial of permission for your child to utilize the District's electronic communications system.

Sincerely,

Michael Perez
Technology Director

COMUNICACION ELECTRONICA Y ADMINISTRACION DE DATOS

Queridos padres,

A su hijo(a) se le ha dado el privilegio de participar en el sistema electrónico de comunicaciones de Distrito y necesita su permiso para poder ingresar al programa. Su hijo(a) podrá comunicarse con otras escuelas, colegios, organizaciones, e individuales alrededor del mundo por medio del “Internet” y otros sistemas/ cadenas de informacion electronica.

El “Internet” es una cadena. Por medio del sistema electrónico de comunicaciones, su hijo(a) tendra acceso o cienes de datos, bibliotecas y servicios de computadoras alrededor del mundo.

Con esta oportunidad educacional también hay responsabilidad. Es muy importante que usted y su hijo(a) léan la póliza, el reglamento administrativo, y forma de aprobación para que puedan hablar de estos requisitos juntos. Uso impropio del sistema resultará en la pérdida del uso de este instrumento educacional.

Por favor note que el “Internet” es una asociación de cadenas diversas en comunicación e información. Es posible que su hijo(a) cruze areas de contenido adulto y material que usted pueda encontrar desagradable, censurable o molesto. Aunque el Distrito tomará pasos razonables para controlar las actividades y no incitamos tal acceso, no es posible para nosotros prevenir en absoluto tal acceso.

El Distrito escolar de Fabens, publica una variedad de proyectos de maestros y estudiantes en la red mundial. Si el trabajo de su hijo(a) es escogido para publicarse, usted debe dar o negar el permiso para que el trabajo del estudiante pueda ser publicado en la página del Distrito de Fabens en la red mundial.

Por favor regrese la forma de aprobación indicando si le da o le niega el permiso a su hijo(a) para participar en el sistema electrónico de comunicaciones.

Sinceramente,

Michael Perez
Director de Tecnologia

EXHIBIT B

STUDENT AGREEMENT FOR ACCEPTABLE USE OF THE ELECTRONIC COMMUNICATIONS SYSTEM

You are being given access to the District's electronic communications system. Through this system, you will be able to communicate with other schools, colleges, organizations, and people around the world through the Internet and other electronic information systems/networks. You will have access to hundreds of databases, libraries, and computer services all over the world.

With this educational opportunity comes responsibility. It is important that you read the District policy, administrative regulations, and agreement form and ask questions if you need help in understanding them. Inappropriate system use will result in the loss of the privilege to use this educational tool.

Please note that the Internet is a network of many types of communication and information networks. 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 will be your responsibility to follow the rules for appropriate use.

CONSEQUENCES FOR INAPPROPRIATE USE

- **Non-Severe Violation:** Student will lose computer privileges/Internet access until a parent conference. Further loss of privilege and length of time will be determined by the administration.
- **Severe Violation:** Pattern of abuse of Non-Severe Violations or Severe violations: Any student who, after Non Severe Violation warning, continues to engage in serious or persistent misbehavior by violating the District's previously communicated written standards of conduct may be removed from class and recommended for suspension.
- **Extremely Violation:** Expellable offense: Student may be expelled from school if he or she engages in conduct on the Internet that contains the elements of the offense of criminal mischief, as defined by State and Federal law. Expulsion may be considered in Extreme violations that blatantly corrupt the educational value of computers or the Internet, or

instances when students have used the Fabens Network access to violate the law or to compromise another computer network (hacking).

The student agreement must be renewed each academic year.

STUDENT

Name _____ ID: _____ Grade _____

School _____

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

I have read the District's electronic communications system policy and administrative regulations and agree to abide by their provisions. I understand that violation of these provisions may result in suspension or revocation of system access.

Student's signature _____ Date _____

EXHIBIT C

EMPLOYEE AGREEMENT FOR ACCEPTABLE USE OF THE ELECTRONIC COMMUNICATIONS SYSTEM

You are being given access to the District's electronic communications system. Through this system, you will be able to communicate with other schools, colleges, organizations, and people around the world through the Internet and other electronic information systems/networks. You will have access to hundreds of databases, libraries, and computer services all over the world.

With this opportunity comes responsibility. It is important that you read the District policy, administrative regulations, and agreement form and ask questions if you need help in understanding them. Inappropriate system use will result in the loss of the privilege of using this educational and administrative tool.

Please note that the Internet is a network of many types of communication and information networks. It is possible that you may run across some material you 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 will be your responsibility to follow the rules for appropriate use.

CONSEQUENCES FOR INAPPROPRIATE USE

* Non-Severe Warning: Employee will lose computer privileges/Internet access until a supervisor conference. Further loss of privilege and length of time will be determined by the supervisor.

* Severe: Pattern of abuse of Non-Severe Violations or flagrant violations: Any employee who, after Level I warning, continues to engage in serious or persistent misbehavior by violating the District's previously communicated written standards of conduct may be removed from work area and recommended for immediate dismissal.

* Extremely Severe: Dismissible offense: Employee may be dismissed from work area if he or she engages in conduct on the Internet that contains the elements of the offense of criminal mischief, as defined by State and Federal law. Employment termination may be considered in flagrant violations that blatantly

corrupt the educational value of computers or the Internet, or instances when employees have used Fabens Internet access to violate the law or to compromise another computer network (hacking).

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

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

I hereby acknowledge that I have received, read, and understand the Fabens ISD Acceptable Use Policy.

Print Name

Department/School:

Signature:

Date:

EXHIBIT D

AGREEMENT FOR ACCEPTABLE USE OF THE ELECTRONIC COMMUNICATIONS SYSTEM BY A NONSCHOOL USER

You are being given access to the District's electronic communications system. Through this system, you will be able to communicate with other schools, colleges, organizations, and people around the world through the Internet and other electronic information systems/networks. You will have access to hundreds of databases, libraries, and computer services all over the world.

With this opportunity comes responsibility. It is important that you read the District policy, administrative regulations, and agreement form and ask questions if you need help in understanding them. Inappropriate system use will result in the loss of the privilege to use this educational tool.

Please note that the Internet is a network of many types of communication and information networks. It is possible that you may run across some material you 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 will be your responsibility to follow the rules for appropriate use.

CONSEQUENCES FOR INAPPROPRIATE USE

- * Suspension of access to the system;
- * Revocation of the computer system account; or
- * Other legal action, in accordance with applicable laws.

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

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

Signature _____ Date _____

EXHIBIT E

PARENT OR GUARDIAN RELEASE FORM

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

I do not give permission for my child to participate in the District's electronic communications system.

I give permission for my child to participate in the District's electronic communications system and certify that the information contained on this form is correct.

I also, give my permission for the items checked below to be displayed on the Fabens ISD web site.

- Original Work
- Name and Grade Level and Campus Information
- Photograph

Signature parent or guardian _____ Date _____

Student Information:

Name _____ ID: _____ Grade _____

School _____

Please note if you would like a complete copy of the Fabens ISD Acceptable Use Policy you can download it off of your district web site at www.fabensisd.net or please contact the Fabens ISD Technology department at (915) 764-2670.

Thankyou.

EXHIBIT F

Request To Unblock Website

Date: _____

Campus/Department: _____

Name: _____

Requested URL (Website): www._____

Website Description:

Requested By Signature: _____

Administrator's Signature: _____

For Technology Department Use:

Approved By: _____ ***Date:*** _____