USER AGREEMENT FOR ACCEPTABLE USE OF THE ELECTRONIC COMMUNICATION SYSTEMS AND INFORMATION RESOURCES

The Veribest Independent School District (the "District") is pleased to make available to employees (faculty, staff, consultants, contractors, temporary-hires, and others), students, and approved parent users access to the interconnected computer information systems within the District (the "Network") and to the world-wide network that provides various means of accessing significant and varied materials and opportunities (commonly known as the "Internet"). (This User Agreement applies to employees if and when they are granted access. That access may be granted to the extent that the District determines appropriate, based on the specific employee's job duties or other factors.)

In order for the District to be able to continue to make its Network and the Internet access available, all users must take responsibility for appropriate and lawful use of this access. Users must understand that one person's misuse of the District technology hardware or software, Network and/or the Internet access may jeopardize the ability of all to enjoy this access. While the District's management and Network administrators will make reasonable efforts to administer use of the Network and Internet access, they must have user cooperation in exercising and promoting responsible use of this access.

This document is the Electronic Communication Systems and Information Resources Acceptable Use Policy (the "Policy" or "AUP") of the District and also relates to Internet and other access or service providers (collectively, the "Provider") as they provide resources necessary for the District to provide the Network and Internet access. Upon accepting your account information, you are agreeing to follow this Policy, and you will then be given the opportunity to enjoy Network and Internet access. If you have any questions about this Policy, you should contact the District Technology Department.

If any user (that is, you or anyone whom you allow to use your account—which itself is a violation) using your account violates this Policy, your access will be denied or withdrawn. Students who violate the policy also will be subject to school discipline; employees will be subject to additional disciplinary action, up to and including, termination

1. Personal Responsibility

a. By accepting your account password and other information from the District and accessing the Network or the Internet, you are agreeing to follow the rules in this Policy. You are also agreeing to report any misuse of access to the Network or the Internet to your building principal or division head. Misuse means any violations of this Policy, or any other use that, while not included in this Policy, has the effect of harming another or another's property.

b. You are responsible for any activity that occurs under the use of your account login. If you leave your device or user account unattended and logged in with the device unlocked, and inappropriate activity occurs, you may be held responsible for that activity. You may not give your login information to another user. (Exception: you may provide it to technical support personnel for tech support purposes but then you are responsible for changing your password after they assist you and resolve your issue.) You may not log into a computer or program and allow another user to utilize your account.

c. If you utilize school District equipment and/or software outside of the District, you must still follow the Veribest ISD Technology AUP rules while utilizing the school District's resources. (example: if you take a laptop home or offsite and access the internet, it is forbidden to surf for porn, gambling, etc.)

2. Unauthorized Equipment Installation

Personal or other purchased equipment not expressly authorized by the Director of Technology or designee will not be installed on the Network. Prohibited equipment is defined as any network attached items including, but not limited to: hubs, switches, routers, wireless access points, splitters, network printers, key loggers, and personal PCs, laptops. Additions of any type of these items are prohibited. Persons who introduce these devices on the Network will be subject to denial of access, and disciplinary actions, including termination for employees.

3. Term of the Permitted Use

After you have been granted access and as long as you follow this Policy, you will have Network and Internet access during the term of your enrollment or employment with the District. (Please be aware that the District may suspend access at any time for technical, policy, failure to sign and return the AUP receipt form or student handbook receipt form or other reasons.)

4. Purpose and Use

a. Veribest ISD Technology Hardware and Software, Network, Internet Access and any other technology related items are provided to staff and students primarily for official business use. Misuse can result in disciplinary actions and possibly termination. If you have any doubt about whether a contemplated activity is appropriate for District business purposes, you may consult with your building principal or division head to help you decide if a use is appropriate.

b. Remember, access to Veribest ISD computer resources is a privilege, not a right. Failure to comply with the guidelines set out in the AUP may result in suspension of access or termination of privileges and other disciplinary action consistent with District policies. Student users should refer to the Student Code of Conduct for a detailed description of the consequences of improper use of the computer system.

5. Computing and Software Usage

a. Software will be used only in accordance with its license agreement. Unless otherwise provided in the license, any duplication of copyrighted software, except for backup and archival purposes by the Technology Director or designee, is a violation of copyright law. In addition to violating copyright law, unauthorized duplication of software is contrary to the District's standards of conduct. The following points are to be followed to comply with software license agreements:
    1. All users must use all software in accordance with license agreements and the District's software regulation. All users acknowledge that they do not own this software or its related documentation, and, that unless expressly authorized by the software publisher, may not make additional copies except for archival purposes.
    2. The District will not tolerate the use of any unauthorized copies of software or fonts in our school system. Any person illegally reproducing software can be subject to civil and criminal penalties including fines and imprisonment. According to the U.S. Copyright Act, illegal reproduction of software is subject to civil damages of as much as U.S. $100,000 per title infringed, and criminal penalties, including fines of as much as U.S. $250,000 per title infringed, and imprisonment of up to five years. A District user, who makes, acquires, or uses unauthorized copies of software will be disciplined as appropriate under the circumstances. Such discipline may include termination of employment. The District does not condone the illegal duplication of software and will not tolerate it.
    3. No user will give software or fonts to any outsiders, including consultants, suppliers, contractors, and others. Under no circumstances will the District use software that has been brought in from any unauthorized location under the District's policy, including, but not limited to, the Internet, home, friends, and colleagues without approval from the Technology Director

or designee. Any user who determines that there may be a misuse of software within the District will notify the Director of Technology, building principal, and/or division supervisor.

4. All software used by the District on District-owned computers will be purchased through appropriate procedures.
5. Generally, District-owned software cannot be taken home and loaded on an employee's home computer if it also resides on a District computer. If an employee is required to use software at home, the appropriate cost center manager will purchase a separate package and record it as a District owned asset in the software register with the Technology Department. However, some software companies provide in their license agreements that home use is permitted under certain circumstances. If an employee is required to use software at home, he or she must first consult with the Technology Department, unless allowed under the software's license agreement, to determine if appropriate licenses allow for home use. The Technology Department will conduct a yearly audit (at least once a year), of all District PCs and servers, including portables, to ensure that the District is in compliance with all software licenses. Random audits may be conducted as well. Audits may be conducted using an auditing software product. The full cooperation of all users is required during audits.

b. Employee use of handheld computing/communication devices (e.g. personal digital assistants (PDA), smart phones, WAP phones, and other personal communication devices) that use any medium to synchronize, transmit, share, or access files on remote computer or server is permitted with some limitations. Synchronization with Microsoft Outlook calendars, contacts, messages, and notes is permitted. Employees who possess District e-mail accounts may access their account via their handheld computing/communication device. The specific details of this privilege are outlined in the next section.

c. The District is not responsible for maintaining, repairing, or otherwise troubleshooting an employee's personal cellular or other electronic devices. The District is not responsible for damage, corruption, modification, and/or deletion of any personal data stored on any employee-owned handheld computing/communication device. Furthermore, the District makes no guarantees of service quality or access regarding handheld devices. Modems or wireless broadband wireless devices inside or connected to office desktop computers (PCs) are not permitted, unless specifically authorized by the Director of Technology. Home based, mobile and/or telecommuting computers are an exception to this rule.

d. Computer equipment supplied by the District must not be altered or added to in any way (e.g., upgraded processor, expanded memory, or extra circuit boards) without prior knowledge and authorization from the Technology and Information Services Department. Unauthorized system changes or components may be removed by Technology Department. On District-supplied computer hardware, workers must not change the operating system configuration or install new software. If such changes are required, they will be performed by Technology Department personnel.

6. Accessing District Internet, E-mail, or Other District Resources via Cellular Phone or other Handheld Communication Device

a. Employees who choose to access the District's Internet or their own District e-mail accounts on their personal handheld communication device (e.g., cell phone, Palm Pilot, etc.) may do so subject to the following restrictions and requirements.

b. The same standards of proper and professional use of the District Internet and District e-mail system apply (including the entirety of this Policy, as well as any provisions applicable from Board Policy (CQ (LEGAL), CQ (LOCAL)), or Employee Handbook, and any other applicable rules or policies) regardless of whether the District services at issue are accessed via District computer or personal device.

c. Use of personal cell phones or other handheld communication devices for business purposes should be limited. Employees are expected to conduct themselves in a professional manner when corresponding as employees of the District, and failure to do so may result in disciplinary action where the behavior or conduct is school related (example: sending threatening text messages to a coworker from a personal cell phone).

d. Although employees are permitted to use their cell phones to access District e-mail and for other acceptable business purposes, a cell phone should not be used in place of the employee's District computer or telephone. Personal cell phones may be used for school business calls, including parent contacts, only during planning periods and other off-duty times during the work day. [See Employee Handbook]. Personal cellular phones should be used for school business only when District telephone and computer access is not readily available. Employees who use other functions of personal cell phones for business purposes (e.g., sending text messages to other employees concerning business, or sending text messages or e-mail containing personally identifiable student information), should limit such use to those instances when other forms of communication are not readily available. An employee who allows the use of his or her cell phone to interfere with the performance of job duties may be subject to discipline. [Consult Employee Handbook for consequences of such conduct].

e. The District strongly encourages employees who choose to use personal communication devices for business purposes to protect those devices with "password protection", blocking any unauthorized users access to its contents. An employee who accesses his or her District e-mail from a cell phone should make a report to the District Technology Department immediately if the cell phone is lost or stolen. The possibly delicate and/or confidential information which could be present on the cell phone is of immediate concern to the District.

f. Electronic mail transmissions and other use of the District's electronic communications system by students and employees shall not be considered private. The District reserves the right to monitor access to and use of District email, District Internet, or other network or computer-related activity, engage in routine computer maintenance and housekeeping, carry out internal investigations, prepare responses to requests for public records, or disclose messages, data, or files to law enforcement authorities. Monitoring shall occur at any time to ensure appropriate use.

g. Reminder: As an employee of a public school district, your communications regarding District business may be subject to public information act requests. Consider this possibility before sending any communication from a cell phone, or other similar device, which contains information or issues of District business.

7. Networking and Internet Usage

a. Employees using District accounts are acting as representatives of Veribest ISD. As such, employees should act accordingly to avoid damaging the reputation of the school District. The introduction of viruses, spyware, adware, malware, any malicious code or tampering with any computer system, is expressly prohibited. Files that are downloaded from the Internet must be scanned with virus detection software before installing or execution. All appropriate precautions should be taken to detect for a virus and, if necessary, to prevent its spread.

b. The truth or accuracy of information on the Internet and in e-mail should be considered suspect until confirmed by a separate (reliable) source. Users shall not place Veribest ISD material (copyrighted software, internal correspondences, etc.) on any publicly accessible Internet computer without proper permission. Alternate Internet Service Provider (ISP) connections (such as AOL dial-up) to the District's internal network are not permitted unless expressly authorized and properly protected by a firewall or other appropriate security device(s).

c. Unless otherwise noted, all software on the Internet should be considered copyrighted work. Therefore, users are prohibited from downloading software and/or modifying any such files without permission from the copyright holder.

8. Electronic Messaging Communications and Voice Mail Systems

a. The District's voice communications and voice mail systems are designed to assist us in better serving stakeholders, enhancing internal communications, and reducing unnecessary paperwork. These guidelines should govern your use of District equipment, with special attention to unified messaging (email, voice mail, facsimiles and video mail.)

b. Privacy is not assured in e-mail, facsimiles, video mail, or voice mail messages, whether a password is used or not. The Telecommunications Manager must have access to all program related passwords at all times, to ensure necessary access to the system. Misuse of passwords or the unauthorized use of another employee's password will result in disciplinary action, up to and including termination. The District may access all employees' messages at any time.

c. E-mail messages are like paper documents: Ask yourself whether you would want anyone else knowing about the content, or whether a conversation would be more appropriate.

d. Reminder: E-Mail is subject to public information act requests (PIA) and is admissible in court in some cases. Keep in mind when you compose an e-mail message that it could possibly be read by anyone or could appear in the local newspaper if requested via a PIA request.

e. Be careful when sending sensitive data via e-mail. It may need to be password protected and possibly encrypted. Review the requirements of HIPAA and FERPA laws which prohibit disclosure of certain student information. Electronic/Voice mail usage must conform to the District's policies against harassment and discrimination. Messages containing defamatory, obscene, offensive, or harassing information, or messages that disclose personal information without authorization, are prohibited. If you receive such unsolicited messages, you are to delete them promptly and not forward them.

f. Chain-type messages and executable graphics also should be deleted and not forwarded---they cause overload on our network system. Employees engaging in the transmission of inappropriate electronic messaging, as determined by the District, will be subject to discipline, up to and including termination. For further information regarding the District's policy against sexual and other unlawful harassment, refer to the student code of conduct or the employee manual.

g. When using e-mail, users should use "e-mail etiquette." For example, avoid the use of all capital letters, as this is considered to be shouting at someone electronically. If you create private mail groups, it is your responsibility to review them periodically so they remain current. The Technology Department will have responsibility for generating and maintaining public mail distribution lists.

h. Users should be mindful of District regulations regarding e-mail retention periods. It is your responsibility to archive any messages that you do not wish to be automatically deleted.

i. E-mail and Internet access should not be overused or misused. Misuse of electronic access (i.e., work time spent online for personal use, copying or downloading copyrighted materials, visiting inappropriate sites, online banking, day trading/stock trading, online dating, online gambling, participating in online auctions, etc.) may result in discipline.

j. Employees and vendors must not make arrangements for, or actually complete installation of voice or data lines with any carrier, if they have not first obtained approval from the Director of Technology or designee.

9. Information Security and Access

a. All users (including third parties) are responsible for the activity performed with their personal user-IDs, whether or not these user-ID's are connecting via external network facilities. User-IDs must never be shared with associates, friends, family members, or others. User-IDs may not be utilized by anyone but the individuals to whom they have been issued. Similarly, users are forbidden from performing any activity with user-IDs belonging to other individuals (excepting authorized anonymous user-IDs like "guest"). With the exception of the District intranet, users must not browse through District computer systems or networks. For example, curious searching for interesting files and /or programs in the directories of other users is prohibited. Steps taken to legitimately locate information needed to perform one's job are not considered browsing. This statement on browsing does not apply to external networks such as the Internet.

b. Confidential information never should be sent over the Internet without the knowledge that it can be intercepted. This includes the transmission of documents containing District financial information, human resource information, student information, or Social Security Numbers. Use extreme caution to ensure that the correct e-mail address is used for the intended recipient(s). If you are sending a document that contains sensitive information, it is recommended that you secure the document; for example, via password, encryption, use of secure socket transfer, etc.

10. Prohibited Use

The user is responsible for his/her actions and activities involving District computers, networks, and Internet services, and for his/her computer files, passwords and accounts. General examples of unacceptable uses which are expressly prohibited include, but are not limited to, the following:

a. Any use that is illegal or in violation of other board policies, including harassing, discriminatory or threatening communications and behavior; violations of copyright laws, etc. - *See Addendum 17: Cyberbullying*;
b. Any use involving materials that are obscene, pornographic, sexually explicit or sexually suggestive;
c. Any inappropriate communications with students or minors;
d. Any use for private financial gain, or commercial, advertising or solicitation purposes;
e. Any use as a forum for communicating by e-mail or any other medium with other school users or outside parties to solicit, proselytize, advocate or communicate the views of an individual or nonschool sponsored organization; to solicit membership in or support of any non-school sponsored organization; or to raise funds for any non-school sponsored purpose, whether profit or not-for-profit.
f. No employee shall knowingly provide school e-mail addresses to outside parties whose intent is to communicate with school employees, students and/or their families for non-school purposes. Employees who are uncertain as to whether particular activities are acceptable should seek further guidance from the building principal or other appropriate administrator.
g. Any communication that represents personal views as those of the District or that could be misinterpreted as such;
h. Downloading or loading software or applications without permission from the system administrator;
i. Opening or forwarding any e-mail attachments (executable, batch, and/or script files) from unknown sources and/or that may contain viruses or malicious software;
j. Sending mass e-mails to District users or outside parties for school or non-school purposes without the permission of the system administrator [or other designated administrator].
k. Any malicious use or disruption of the District's computers, networks, and Internet services or breach of security features;
l. Any misuse or damage to the District's computer equipment;
m. Misuse of the computer passwords or accounts (employees, students, or other users);

n. Any communications that are in violation of generally accepted rules of network etiquette and/or professional conduct, including the use of profanity or vulgar, obscene or sexually explicit language;
o. Any attempt to access inappropriate/unauthorized sites (i.e. Internet/Websites, intranet websites, and/or application servers);
p. Failing to report a known breach of computer security to the system administrator;
q. Executing, using, or viewing any application or website that is resource intensive, resulting in excessive network saturation and denial-of-service for other users;
r. *Users* using District computer networks are prohibited from gaining unauthorized access to any information system or network to which they have not been expressly granted access. *Users* using District computer networks are also prohibited from in any way damaging, disrupting, or interfering with the operations of multi-user information systems to which they are connected. Likewise, *users* are prohibited from capturing or otherwise being in possession of passwords, encryption keys, or any other access control mechanism that has not been expressly assigned to them. *Users* are furthermore prohibited from possessing or using software tools which could provide unauthorized access to system resources (these include password dictionary attack programs, encryption key brute-force discovery programs, and software for defeating copy-protection mechanisms). These actions are defined as “Hacking” and are in direct violation of the District Acceptable Use Policy.
s. Using school computers, networks, and Internet services after such access has been denied or revoked;
t. Any attempt to delete, erase, or otherwise conceal any information stored on a school computer that violates these rules;
u. Use that violates this Policy, the student code of conduct or the employee standards of conduct;
v. Unauthorized disclosure, use, or distribution of personally identifiable information or personal identification regarding students or employees;
w. Personal or political use to advocate for or against a candidate, office-holder, political party, or political position. Research or electronic communications regarding political issues or candidates shall not be a violation when the activity is to fulfill an assignment for class credit;
x. Participating in chat rooms other than those approved, sponsored and/or overseen by the District;
y. and/or the use of personal devices such as PDA’s (Palms, Visors, cell phones with web capability, etc.) and laptops (either wireless or Ethernet) or any device used to access Veribest ISD Networks is prohibited unless this Policy provides otherwise.

11. No Expectation of Privacy

a. Electronic mail transmissions and other use of the electronic communications system by students and employees shall not be considered private. Employees have no expectation of privacy in their use of District computing and network resources, including electronic messaging (e-mail), online chatting, any stored files, etc.

b. The District reserves the right to monitor, track, and report access to and use of District e-mail, the Internet, or other network or computer-related activity, engage in routine computer maintenance and housekeeping, carry out internal investigations, prepare responses to requests for public records, or disclose messages, data, or files to law enforcement authorities. Monitoring by designated District staff shall occur at any time to ensure appropriate use.

12. Confidentiality of Information

Employees are expected to use appropriate judgment and caution in communications concerning students and staff to ensure that personally identifiable information remains confidential. When engaging in written communication regarding any student, employees should avoid using the student’s name or ID number, and instead should use the student’s initials if possible.

13. Staff Responsibilities to Students

Teachers, staff members, and volunteers who use District computers for instructional purposes with students must supervise such use. Teachers, staff members and volunteers are expected to be familiar with the District's policies and rules concerning student computers and Internet use and to enforce them. When, in the course of their duties, employees/volunteers become aware of student violations, they are expected to stop the activity and inform the building principal [or other appropriate administrator].

14. Compensation for Losses, Costs and/or Damages

Users shall be responsible for any losses, costs or damages incurred by the District related to violations of policy CQ and/or these rules.

15. No Responsibility for Unauthorized Charges, Costs, or Illegal Use

The District assumes no responsibility for any unauthorized charges made by users, including but not limited to credit card charges, subscriptions, long distance charges, equipment and line costs, online gambling charges or debts, or for any illegal use of its computers such as copyright violations. Therefore, the District will hold the user liable for the user's actions.

16. Addendum: Policy on Social Media for School Employees

In accordance with (IAW) **DH(Local)-X** *(Employee Standards of Conduct)***, issued 8/11/2010**.

a. Computer Use and Data Management (Policy CQ)

1. Access to the District's electronic communications system, including the Internet, is available to employees for instructional and administrative purposes and in accordance with administrative regulations. Access to the District's electronic communications system is a privilege, not a right. All users will be required to acknowledge receipt and understanding of all administrative regulations governing use of the system and will agree in writing to allow monitoring of their use and to comply with such regulations and guidelines. Noncompliance may result in suspension of access or termination of privileges and other disciplinary action consistent with District policies. Violations of law may result in criminal prosecution as well as disciplinary action by the District. For a complete listing of the Veribest ISD technology acceptable use policy, please access the following link: http://www.veribestisd.net/

2. Electronic mail transmissions and other use of the electronic communications system by employees are not private and may be monitored at any time by designated District staff to ensure appropriate use.

b. Personal Use of Electronic Media (Policy DH)

1. 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 Web sites (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.

2. 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 duties, 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.

3. An employee who uses electronic media for personal purposes shall observe the following:

    a. The employee may not set up or update the employee's personal social network page(s) using the District's computers, network, or equipment.

    b. The employee shall not use the District's logo or other copyrighted material of the District without express, written consent.

    c. 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:

    d. Confidentiality of student records. [See Policy FL]

    e. Confidentiality of health or personnel information concerning colleagues, unless disclosure serves lawful professional purposes or is required by law. [See Policy DH (EXHIBIT)]

    f. Confidentiality of district records, including educator evaluations and private e-mail addresses. [See Policy GBA]

    g. Copyright law [See Policy EFE]

    h. Prohibition against harming others by knowingly making false statements about a colleague or the school system. [See Policy DH (EXHIBIT)]

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

c. Use of Electronic Media with Students (Policy DH)

1. A certified or licensed employee, or any other employee designated in writing by the superintendent, assistant superintendent, or a campus principal, may communicate through electronic media with students who are currently enrolled in the District. The employee must comply with the provisions outlined below. All other employees are prohibited from communicating with students who are enrolled in the District through electronic media.

2. 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.

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

    a. *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 Web sites (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.

b. *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.

c. *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.

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

a. 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.

b. 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.)

c. 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.

d. The employee shall not communicate directly with any student between the hours of 10 p.m. and 6 a.m., unless an extracurricular emergency exists. An employee may, however, make public posts to a social network site, blog, or similar application at any time.

e. The employee does not have a right to privacy with respect to communications with students and parents.

f. 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:

1. 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]

2. Copyright law [Policy EFE]

g. Prohibitions against soliciting or engaging in sexual conduct, a romantic relationship, or other inappropriate social relationship with a student. [See Policies DF and DH]

h. 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.

i. Upon written request from a parent or student, the employee shall discontinue all forms of electronic one-to-one communication with students. 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 with an explanation of the need for the exception.

d. User Acknowledgement Required

Each user authorized to access the District computers, networks, telecommunications, and Internet services is required to sign an acknowledgement form (CQ Exhibit D), or the Employee or Student Handbook stating that they have read policy CQ and these rules. As a condition of continued employment, employees, consultants, and contractors must annually sign an acceptable usage policy or Veribest ISD Employee or Student Handbook. The acknowledgement form will be retained in the employee's personnel file or in the Technology Department's files. Agreements from students will be maintained in campus records, as will Agreements from parents and volunteers.

17. Addendum: Cyber Bullying

In accordance with (IAW) **CQ (Legal)** *(Electronic Communication and Data Management)***, issued 8/11/2010** and (*The Children's Internet Protection Act);* in compliance with Texas House Bill 2003.

Texas House Bill No. 2003 - A BILL TO BE ENTITLED AN ACT: relating to the creation of the offense of online harassment.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF TEXAS:

SECTION 1. Chapter 33, Penal Code, is amended by adding Section 33.07 to read as follows:

Sec. 33.07. ONLINE HARASSMENT.

(a) A person commits an offense if the person uses the name or persona of another person to create a web page on or to post one or more messages on a commercial social networking site:

(1) without obtaining the other person's consent; and

(2) with the intent to harass, embarrass, intimidate, or threaten any person.

(b) A person commits an offense if the person sends an electronic mail, instant message, text message, or similar communication that references a name, domain address, phone number, or other item of identifying information belonging to any person:

(1) without obtaining the other person's consent; and

(2) with the intent to cause a recipient of the communication to reasonably believe that the other person authorized or transmitted the communication.

(c) An offense under this section is a Class A misdemeanor, except that the offense is a felony of the third degree if the actor commits the offense with the intent to harm or defraud another.

(d) If conduct that constitutes an offense under this section also constitutes an offense under any other law, the actor may be prosecuted under this section, the other law, or both.

(e) In this section:

(1) "Commercial social networking site" means any business, organization, or other similar entity operating a website that permits persons to become registered users for the purpose of establishing personal relationships with other users through direct or real-time communication with other users or the creation of web pages or profiles available to the public or to other users. The term does not include an electronic mail program or a message board program.

(2) "Identifying information" has the meaning assigned by Section 32.51.

SECTION 2. This Act takes effect September 1, 2009.

18. Addendum: Protecting Children in the 21st Century Act Amendment

- To become effective July 1st, 2012 for the school year 2012-2013 for all Texas Schools.

Schools and Libraries Universal Service Support Mechanism; Implementation of the Protecting Children in the 21st Century Act Amendment to Section 254(h) of the Communications Act of 1934; Report and Order**: FCC 11-125**, Released: August 11, 2011.

a. Under the schools and libraries universal service support mechanism (also known as the E-rate program), eligible schools, libraries, and consortia that include eligible schools and libraries may apply for discounted eligible telecommunications, Internet access, and internal connections services. Currently, the Universal Service Administrative Company (USAC) is the administrator of the E-rate program and processes the applications for discounted services. School and library applicants that seek to receive discounts on Internet access or internal connections have been required to certify their compliance with the Children's Internet Protection Act (CIPA) since 2001. Congress adopted CIPA in 2001 as part of the Consolidated Appropriations Act, 2001. Pub. L. No. 106-554. CIPA amended section 254(h) of the Communications Act of 1934, as amended, 47 U.S.C. §§ 151 et seq.

b. CIPA requires schools and libraries that seek E-rate discounts for Internet access and internal connections to certify that they have in place certain Internet safety policies and technology protection measures. As required by CIPA, section 54.520(c) of the Commission's rules requires that school and library Internet safety policies must include a technology protection measure that protects against Internet access by both adults and minors to visual depictions that are (1) obscene; (2) child pornography; or, with respect to use of the computers by minors, (3) harmful to minors. In addition, section 54.520(c)(1)(i) requires a school to certify that its Internet safety policy includes "monitoring the online activities of minors." Applicants make their CIPA certifications on the Receipt of Service Confirmation Form (FCC Form 486), or the Certification by Administrative Authority to Billed Entity of Compliance with the Children's Internet Protection Act (FCC Form 479).

c. In the Report and Order in this proceeding, the Commission added the statutory language from the Protecting Children in the 21st Century Act, a statutory amendment to CIPA, regarding the education of students about appropriate online behavior, to the existing Commission rules implementing CIPA. (Protecting Children in the 21st Century Act, Pub. L. No. 110-385, Title II, 122 Stat. 4096 (2008)). Specifically, the Protecting Children in the 21st Century Act directs E-rate applicants to certify that their CIPA-required Internet safety policies provide for 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. This requirement is applicable to schools only. The Commission implemented this statutory language verbatim at 47 C.F.R. section 54.520(c)(1)(i). The last sentence of that rule now states that "[b]eginning July 1, 2012, schools' Internet safety policies must provide for educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyber bullying awareness and response." The Commission also took the opportunity to make minor non-substantive revisions to Commission rules to conform to existing statutory language from the CIPA statute where necessary and two corrections to the Commission's *Schools and Libraries Sixth Report and Order* (FCC 10-175).

d. The Commission amended **section 54.520(c)(1)(i)**, and made minor amendments to the Commission's rules with regard to CIPA, to conform with statutory language as follows:

1. The Commission revised section **54.520(c)(1)(i)** to include the new certification requirement added by the Protecting Children in the 21st Century Act. This provision requires a certification that a school's Internet safety policies provide for the education of minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyber bullying awareness and response. It declined to define or interpret the terms provided in the new statutory language, such as "social networking" or "cyber bullying."
2. The Commission revised section **54.500(k)** to make it consistent with the statute that a secondary school is "a nonprofit institutional day or residential school, including a public secondary charter school, that provides secondary education, as determined under State law, except that the term does not include any education beyond grade 12." It also revised sections **54.501(a)(1)**, **54.503(c)(2)(i)**, and **54.504(a)(1)(i)** to refer consistently and identically to section **54.500** definitions of elementary and secondary schools.
3. The Commission revised section **54.520(a)(1)** to add "school board" to the definition of entities that are subject to CIPA certifications. Although section **254(h)** of the Act includes the term "school board" as an entity to which the CIPA certifications may apply, the existing rules do not include this term.
4. The Commission revised section **54.520(a)(4)** to add the existing statutory definitions of the terms "minor," "obscene," "child pornography," "harmful to minors," "sexual act," "sexual contact," and "technology protection measure," consistent with the statute.
5. The Commission revised sections **54.520(c)(1)(i)** and **54.520(c)(2)(i)** – consistent with sections **254 (h)(5)(B)(ii), (h)(5)(C)(ii), (h)(6)(B)(ii),** and **(h)(6)(C)(ii)** of the Act – to state that a school or library must enforce the operation of technology protection measures while the school or library computers with Internet access are being used.
6. The Commission revised sections **54.520(c)(1)(i)** and **54.520(c)(2)(i)** to reflect language in sections **254(h)(5)(D)** and **(h)(6)(D)** of the Act that permits an administrator, supervisor, or other person authorized by the certifying authority to disable an entity's technology protection measure to allow for bona fide research or "other lawful purpose by an adult."
7. The Commission added section **54.520(c)(4)** to require local determination of what matter is inappropriate for minors. Although this is mandated by the statute, it had not been codified.
8. The Commission added a rule provision requiring each Internet safety policy that is adopted pursuant to section **254(l)** of the Act to be made available to the Commission upon request. Although this requirement is mandated by the statute, it had not been codified.
9. The Commission revised sections **54.520(c)(1)(iii)(B), (c)(2)(iii)(B)**, and **(c)(3)(i)(B)** to clarify that, in the first year of an entity's participation in the E-rate program only, the entity's Administrative Authority may certify on the FCC Form 486 or 479 that it will complete all CIPA requirements by the following funding year and still receive funding for the current funding year.
10. The Commission also added a rule provision at **54.520(h)** requiring a local public notice and a hearing or meeting to address any Internet safety policies newly adopted pursuant to CIPA. Although this is mandated by the statute and was discussed in the *CIPA Order*, it had not been codified. The requirement only applies to an entity that has no previous Internet safety policy or did not provide public notice and a hearing or meeting when it adopted its Internet safety policy. Unless required by local or state rules, an additional public notice and a hearing or meeting is not necessary for amendments to Internet

safety policies, including the changes to schools' Internet safety policies required by the Protecting Children in the 21st Century Act

e. The Commission made several additional clarifications or findings pertaining to CIPA:

1. As required by CIPA, section **54.520(c)** of the Commission's rules requires that school and library Internet safety policies must include a technology protection measure that blocks visual depictions that are (1) obscene; (2) child pornography; or, with respect to use of the computers by minors, (3) *harmful to minors*.
2. The statute provides that "[a] determination of what matter is inappropriate for minors is one that should be made by the school, school board, local educational agency, library, or other authority responsible for making the determination." **47 U.S.C. § 254(l)**.
3. In the Report and Order, the Commission clarified that although individual Facebook or MySpace pages could potentially contain material harmful to minors, it did not find that these websites are *per se* "harmful to minors" or fall into one of the categories that schools and libraries must block.
4. The Commission also determined that the maintenance of the Internet safety policy should be in accordance with the existing audit and recordkeeping requirements of rule section 54.516(a) and existing certification number 10 on the FCC Form 486, which require schools and libraries to retain documents for at least five years after the last day of service delivered in a particular funding year.
    a. The Commission determined that USAC should give applicants the opportunity to correct minor errors that could result in violations of the Commission's CIPA rules before instituting recovery of E-rate funds, but such errors must be immaterial to statutory CIPA certification compliance.
    b. The Commission took the opportunity to make minor corrections to the *Schools and Libraries Sixth Report and Order* (**FCC 10-175**).
        i. In the discussion of dark fiber in the *Sixth Report and Order*, the seventh sentence in paragraph 9 read: "We emphasize that selecting a telecommunications carrier as a service provider does not absolve schools and libraries of their obligation to adhere to the **Children's Internet Protection Act (CIPA)** requirements when they use that service to obtain Internet service or access to the Internet." The Commission revised the last part of that sentence to read: ". . . when they use USF funding to obtain discounted Internet access service."
        ii. The Commission also corrected **54.507(g)(1)(i)** of the final rules to the *Schools and Libraries Sixth Report and Order* to change "Schools and Libraries Corporation" to "Administrator" and to reflect that voice mail, although eligible for E-rate discounts, does not need to be listed as an individual eligible service in our rules. The revised rule states: "**(i)** The Administrator shall first calculate the demand for services listed under the telecommunications services, telecommunications, and Internet access categories on the eligible services list for all discount levels, as determined by the schools and libraries discount matrix in **§ 54.505(c)**. These services shall receive first priority for the available funding."

f. The certification required by the Protecting Children in the 21st Century Act requires a school to adopt an Internet safety policy or amend an existing Internet safety policy that, among the other requirements for:

a. CIPA, provides for educating minors about appropriate online behavior. This certification, which includes the appropriate online behavior for interacting with other individuals on social networking websites and in chat rooms and cyber bullying awareness and response**, is required only of schools beginning July 1, 2012.**

b. When schools certify their compliance with CIPA, by filing FCC Forms 486 or 479, they will also be providing a certification that their Internet safety policies provide for the education of minors about appropriate online behavior.
c. In order to make this certification, they will have needed to update their Internet safety policies with the plan they are using to provide education about appropriate online behavior.

g. Veribest Independent School District (VISD) Provisions for Internet Safety Awareness Training

Veribest Independent School District will provide **Internet Safety** Information training annually, via one of the following venues:

1. Classroom instruction by the teacher using the **Internet Safety** presentation included on the Network Video L:ibrary; or
2. Presentation of the **Internet Safety** video at a scheduled elementary and secondary assembly for this purpose.
3. Conducted training will be documented and attendees noted to comply with and remain in accordance with Texas State and Educational Agency guidelines.

19. Addendum: Veribest ISD Bring Your Own Device (BYOD) Policy

a. Veribest School District will now be incorporating the use of such items as personal laptops and tablets with browsing capabilities and/or educational apps and software. As with other personally owned items, the school shall not be held liable for the loss, damage, misuse, or theft of personally owned devices brought to school.

b. This policy is not intended as a requirement that any (student)-(faculty or staff) bring personal technology to school. All (students)-(faculty or staff) will continue to be able to utilize school equipment. No student will be left out of the instruction process.

c. A personally owned device is defined as one with:
1. Academic applications and functions
2. Online capabilities
3. Digital, audio and/or video recording.

d. Examples of a personally owned device shall include but are not limited to: iPads, iPhone, iPods, Nooks, Kindle, Kindle Fire, and other tablet PCs; laptop computers; camcorders; and digital cameras. Specific examples of devices that will NOT be permitted are gaming devices (example: Nintendo DS) and laser pointer devices.

e. (Students)-(Faculty or staff) are granted the limited right to use their personally owned technology resources at Veribest School District upon return of this signed *Veribest School District Bring Your Own Device (BYOD) Policy*.

f. To ensure the learning and safety of all of our (students)-(faculty or staff), Veribest School District (students and parents)-(faculty or staff) agree to both read, acknowledge, and follow these guidelines:

1. Devices are for educational use. During school hours (students)-(faculty or staff) may not use their devices to make phone calls, play games, text, or access any social networks. Violations of this policy will result in loss of use and escalating consequences, as determined by the District Administration. In addition to disciplinary action, the (students) phone or device will be confiscated and returned only to a parent/guardian.

2. Should a legitimate need arise during the school day, office phones may be used to contact a parent once permission is granted by office personnel. (Students) who become ill during the school day are to follow the procedure for contacting a parent, outlined in the Student Handbook.

3. During school hours, devices will be turned on only when permitted by the (teacher)-(administrator).

4. All accessories, cases, screen wallpaper and backgrounds must be school-appropriate.

5. Personally owned devices used in school are not permitted to connect to the Internet through a 3G, 4G or other content service providers. Personally owned devices must access the Internet via the school's content filtered wireless network.

6. Streaming videos from the Internet or YouTube during school hours is permitted only with the direct permission of the (teacher)-(administrator).

7. Any recording device, including but not limited to iPads, video and digital cameras and camera phones to take videos or still pictures, may not be used to slander, bully or denigrate any student, visitor, staff member, faculty member, and or administrator, on or off the campus at any time.

8. All messages or postings to any Internet site on or off campus at any time (notes, email, newsgroups, bulletin boards, wikis, or other interactive forms of communication such as Instant Messaging) shall be educationally purposeful and appropriate. Hate mail, harassment, discriminatory remarks, vulgarity, swearwords, other antisocial behaviors, chain letters, and threats of any kind are prohibited. Appropriate messages would include such communications relating to Veribest School District academics, co-curricular events, and school community life.

9. Users are responsible for all activities conducted when using personal devices and accounts.

10. Users shall respect copyright laws and licensing agreements pertaining to materials entered into and obtained via the Internet or other electronic sources.

11. Use of the Internet and/or other resources for personal gain, profit, commercial advertising, or political lobbying is prohibited.

12. Use of your device must be in support of curriculum and research and consistent with the purposes and *Mission Statement of Veribest School District*.

13. The use of Veribest School District technology resources to purposefully attempt to access pornographic material, inappropriate text files, information advocating violence or files harmful to the integrity of Veribest School District is prohibited.

14. Also restricted is access to information on, but not limited to, gambling, illegal drugs, alcohol use, online merchandising, hate speeches, criminal skills, alternative journals, Fanfic, and chat rooms. Use must be

consistent with the *Mission Statement of Veribest School District* and reflect the accepted moral standards expressed in that Mission Statement.

15. (Students)-(Faculty or staff) may not access social networking sites such as Facebook, Twitter, and Flickr.

16. (Student)-(Faculty or staff) may access school email accounts under the approval of and under the supervision of a teacher, administrator and/or Computer Teacher. Outside email accounts cannot be accessed.

17. Users of the Internet will not give their real name, address, phone number, school name or any personal information to anyone on the Internet unless under the supervision of a teacher or administrator.
    - Example: (Student)-(Faculty or staff) may be asked to provide personal information when signing up for Web 2.0 tools or when registering to access online textbooks and resources.

18. (Students)-(Faculty or staff) making inappropriate references about the school and/or its students, faculty, staff or administrators on any public Internet site, chat rooms, or other public electronic media will be subject to disciplinary action that will be determined by administrators and could include (suspension or expulsion)-(termination of employment).

19. No devices are allowed in the restroom at any time.

20. (Students)-(Faculty or staff) may not use any means to access restricted sites.

21. (Students)-(Faculty or staff) may not record or post images of teachers, staff or other personnel on the Internet without receiving permission from the individual(s) involved.

22. (Students)-(Faculty or staff) may not use the cameras on their iPads unless given permission by and under the direct supervision of a teacher or administrator during school hours. Parents of students may restrict the use of the camera at any other time by setting the Parental Controls.

23. Students are required to have a case for their device at all times, and to transport the device in a safe manner (preferably in a backpack). (Students)-(Faculty or staff) participating in extracurricular activities before, during and after school should keep their device in a secure area. Students are encouraged to use the lockers provided in the athletic facilities with school locks.

g. Consequences of Inappropriate Behavior

1. Any user who does not comply with these guidelines will lose the privilege of bringing their device for a period of time, that period of time to be set at the discretion of the District Administration.

2. (Students)-(Faculty or staff) who have repeated or severe infractions of the policy will be subject to disciplinary action by the District Administration. Violations of federal and state regulations, such as sending threatening email and accessing or distributing obscene material, will be reported to and dealt with by the governing law enforcement agency.

STUDENT USER AGREEMENT & PARENT PERMISSION FORM (CHROMEBOOKS)

Rules and Appropriate Usage

Veribest Independent School District encourages the uses of the internet as a tool for research and education. Chromebooks and other school provided devices and services, like any other school property, must be used for educational purposes for which they are intended. The Chromebooks used by students are the property of Veribest Independent School District. The ability to use a Chromebook by all students is a privilege, not a right, and may be revoked at any time for inappropriate conduct.

USE OF EQUIPMENT (Hardware and Software)

- School Chromebooks are to be used for research, education and school related business ONLY.
- The use of the Chromebook must not violate the existing Acceptable Use Policy or the BYOD section that is currently in the handbook.
- Students may not destroy, deface, or alter Chromebook equipment or files not belonging to the student.
- If the damage of a Chromebook is intentional, willful or purposeful, the parents or guardians will pay the full replacement cost of the Chromebook. Estimated replacement cost of a Chromebook for the 2016 school year is an estimated $200.
- Students may not attempt to hid files or activity on a Chromebook owned by the district.
- **Students are not permitted to install any software on the Chromebooks without consent by the Technology Director or Veribest Faculty and Staff.**

THE NETWORK

- Chat lines, bulletin boards, forums, etc. may not be accessed by students without prior consent from a teacher or person monitoring the Internet use.
- Engaging in online activities that are inappropriate will result in automatic termination of the student's network/Internet privileges in accordance to the handbook.
- Sending messages via school technology with the intent to intimidate, frighten, threaten, or bully another person is considered harassment and will have significant consequences per the handbook.
- Students may not change, alter, or attempt to bypass any Chromebook security measures including filtered Internet sites.
- The Veribest Independent School District has filtering in place to block inappropriate websites and content. All devices are filtered, including the Chromebooks, when connected to an Access Point on campus.

PRIVACY

- It is a violation to share your Chromebook password with anyone else, or to access any account belonging to another student, faculty member, or staff member.

MANAGEMENT

- Since the Chromebooks belong to Veribest Independent School District, the school may monitor all devices and their usage. Veribest Independent School District also reserves the right to search Internet accounts accessed with school equipment without permission if it is felt that illegal or otherwise inappropriate use of technology is occurring. Improper use of Veribest technology devices will result in loss of network/Internet privileges and other consequences as per the handbook.

Student Name: _____ Parent/Guardian Name: _____

Parent Phone Number: _____

Parent/Guardian Signature: _____ Date: _____

Student Signature: _____ Date: _____