Section I:

STAFF ACCEPTABLE USE POLICY
ELECTRONIC COMMUNICATION AND DATA MANAGEMENT REGULATIONS

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

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.

1. 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. 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.

2. SYSTEM ACCESS

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

A. As appropriate and with the written approval of the immediate Supervisor, District employees will be granted access to the District's system.

B. Students in grades Pre-K - 5 will be granted access to the District's system by their teachers, as appropriate. Students in grades 6 - 12 will be assigned individual accounts.

C. A teacher must apply for a system account, and in doing so will be ultimately responsible for use of the account.

D. The District will require that all passwords be changed twice a year.

E. Any system user identified as a security risk or having violated District and/or campus computer use guidelines may be denied access to the District's system.

F. URL filtering and blocking is maintained by the district for protection of minors denying access to inappropriate matter on the Internet, World Wide Web, E-mail, chat rooms and other forms of direct electronic communications. In cases where this filtering fails, the user is required to report the site to the Technology Director immediately so that appropriate internal blocking may be implemented.

G. The district has in place a firewall for protection from unauthorized access or "hacking", and other unlawful activities online. In cases where this protection fails, all users who are aware of this failure are required to report the incident to the Technology Director immediately.

3. TECHNOLOGY DIRECTOR RESPONSIBILITIES

The Technology Director for the District's electronic communications system (or designee) will:

A. Disseminate and enforce applicable District policies and acceptable use guidelines for the District's system.

B. Ensure that all users of the district's system complete and sign an agreement to abide by District policies and administrative regulations regarding such use.

C. Ensure that employees supervising students who use the District's system are provided training emphasizing the appropriate use of this resource.

D. Ensure that all software loaded on computers in the District is consistent with district standards and is properly licensed.

E. Monitor and/or examine all system activities, including electronic mail transmissions, as deemed appropriate to ensure proper use of the system.

F. Establish a retention schedule for messages and files on any District system.

G. Monitor and remove any content deemed inappropriate.

H. Set limits for data storage within the District's system, as needed.

I. Maintain AUP Guidelines for all District Technology.

J. Maintain Policies and Procedures of District owned laptop computer equipment.

K. Maintain WISD Donation Procedure.

4. INDIVIDUAL USER RESPONSIBILITIES

The following standards will apply to all users of the District's electronic information/communications systems:

I. ONLINE CONDUCT

A. The individual in whose name a system account is issued will be responsible at all times for its proper use.

B. The system may not be used for illegal purposes, in support of illegal activities, or for any other activity prohibited by District policy or guidelines.

C. System accounts are not to be shared for any reason.

D. Staff may not distribute personal information about themselves or others by means of the electronic communication system, unless a written release is obtained.

E. System users must maintain electronic mail in accordance with established retention guidelines.

F. System users may not redistribute copyrighted programs or data except with the written permission of the copyright holder or designee. Such permission must be specified in the document or must be obtained directly from the copyright holder or designee in accordance with applicable copyright laws, District policy, and administrative regulations.

G. System users will not be able to download, upload, or run software or shareware without filing an approved "Software Loading Request Form".

H. System users may not send or post Email messages that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation, or the illegal sending of "Chain Letters" or "broadcast messages" (spamming) to lists or individuals, and any other types of use which would cause congestion of the networks or otherwise interfere with the work of others, is prohibited.

I. System users may not intentionally access Web sites that are abusive obscene, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.

J. System users should be aware of the use of school-related electronic mail addresses might cause some recipients or other readers of that mail to assume they represent the District or school, whether or not that was the user's intention.

K. System users may not abuse District resources related to the electronic communications system. System users may not use an electronic mail package or service on school computers, other than that approved by the school district. System users may not use "chat" programs or message boards.

L. System users may not gain unauthorized access to resources or information.

M. System users may not re-configure, remove, replace or alter any District hardware. Likewise, no user may modify and/or remove system settings and/or re-format any District computer.

N. System users may not use the network for personal use such as entering contests, advertising, political lobbying, or commercial activities including online purchasing.

II.VANDALISM PROHIBITED

Any malicious attempt to harm or destroy District equipment or data of another user of the District's system, or any of the agencies or other networks that are connected to the Internet is prohibited. Deliberate attempts to degrade or disrupt system performance are violations of District policy and administrative regulations. These actions may be subject to State and Federal laws. Such prohibited activity includes, but is not limited to, the uploading or creating of computer viruses or harmful program components.

Vandalism as defined above will result in the cancellation of system use privileges and will require restitution for costs associated with system restoration, as well as other appropriate consequences.

III. FORGERY PROHIBITED

Forgery or attempted forgery of electronic mail messages is prohibited. Attempts to read, delete, copy, or modify the electronic mail of other system users, deliberate interference with the ability of other system users to send/receive electronic mail, or the use of another person's user ID and/or password is prohibited.

IV. INFORMATION CONTENT/ THIRD-PARTY 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 user who gains access to such material is expected to discontinue the access as quickly as possible and to report the incident to a supervisor.

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

Employees may participate in a chat room for job related information in accordance with District Policy.

5. DEVELOPMENT OF WEB PAGES

All web pages residing on the Whitehouse Independent School District Web Server, may be reviewed by the Technology Director or designee.

6. NETWORK ETIQUETTE

System users are expected to observe the following network etiquette:

A. Be polite: messages typed in capital letters are the computer equivalent of shouting and are considered rude.

B. Use appropriate language: swearing, vulgarity, ethnic or racial slurs, and any other inflammatory language is prohibited.

C. Pretending to be someone else when sending/receiving messages is prohibited.

D. Transmitting obscene messages or pictures is prohibited.

E. Using the network in such a way that would disrupt the use of the network by other users is prohibited.

7. DONATED EQUIPMENT

All donations must be approved through the " Whitehouse I.S.D. Donation Procedure".

8. USE OF PERSONAL EQUIPMENT

Personal equipment is strictly prohibited from use on the W.I.S.D. private network, but may be allowed on the public network.

9. TERMINATION REVOCATION OF SYSTEM USER ACCOUNT

Termination of an employee's or a student's access for violation of District policies or regulations will be effective on the date the Principal or Technology Director receives notice.

INAPPROPRIATE USES

- Using the system for illegal purposes.
- Borrowing someone's account without permission.
- Posting personal information about yourself or others (such as addresses and/or phone numbers.)
- Downloading or using copyrighted information without permission from the copyright holder.
- Posting messages or accessing materials that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.

- Abusing school resources through the improper use of the computer system.
- Gaining unauthorized access to restricted information or resources.
- Reformatting or reconfiguring any standard hardware or software.

CONSEQUENCES FOR INAPPROPRIATE USE

- Suspension of access to the system;
- Revocation of the computer system account; or
- Other disciplinary or legal action, in accordance with district policy, guidelines and employee handbook.

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 merchant ability 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 of 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.

Section II:

Whitehouse ISD
Acceptable Use Policy Guidelines
For Technology

OVERVIEW OF DISTRICT TECHNOLOGY GOALS:

- To meet the challenge of preparing all students in Whitehouse Independent School District (ISD) for a technologically challenging future by complying with Texas Essential Knowledge and Skills guidelines as set forth by the Texas Legislature.
- To better inform and utilize parents, community, and business leaders in the area of technology implementation.
- Allow technology to be implemented K-12 in a sequentially valid plan that apportions equipment from simple to complex through the grade levels (i.e. Kindergarten should not utilize equipment more advanced than the high school campus.) This policy will require reapportionment and/or migration of equipment at reasonable and predictable intervals.
- To allow students K-12 to become more and more responsible for the use and care of current technology. Elementary students will be taught basic care of input and output devices. Junior high students will learn the computer system components and proper care of each. High school students will be taught to program, manage, and maintain, software and hardware.
- To more profusely Integrate technology tools in the curriculum as students move through the grade levels. New technologies, new techniques, and new skills will accompany each grade level in a logical, sequential, technology-infused curriculum, beginning in Kindergarten with keyboarding skills.
- To commit Whitehouse ISD in providing all students the most effective, current and real-world technologies so that all students may gain valuable, relevant, and marketable skills.
- To utilize technology in the district to meet student instructional needs and District administrative needs. Planning for technology will be driven by instructional objectives, student needs in achievement, curricular and instructional strategies, and administrative assessments for effectiveness.
- Interconnectivity will be the priority of the Technology Plan. The ability to share resources, information, and ideas is one of the most important assets a school district can offer, second only to character development through a nurturing, caring spirit.

STANDARDS:

Whitehouse ISD maintains high standards of ethical and acceptable use of all technology for educational purposes. To accomplish these standards the following policies will be followed:

STAFF & STUDENT TRAINING

Teachers requesting additional computers/technologies will complete the required technology request forms to evaluate the desired outcome from the requested hardware/software. All new equipment to the classroom will require that the teacher be trained on the use of that equipment.

Whitehouse ISD will provide instruction and training in current technologies and infusion techniques applicable to the classroom.

A. Students and staff are required to read and agree to the Whitehouse ISD Acceptable Use Policy
B. A completed Employee/Student AUP Agreement Contract must be on file before an individual network contract can be activated.

IMPLEMENTATION OF TECHNOLOGY

Staff members will be required to maintain ethical and copyright standards in accordance with federal and state laws. No software will be loaded on a machine that has not been approved by the technology director.

The following network policies will apply:

- Access of Network & Internet will be given through student and staff password accounts. Accounts will be maintained by the individual and passwords will not be given or shared with anyone else.
- All use of Whitehouse ISD's Network and technologies must be consistent with policies and goals of the Whitehouse Independent School District, Texas Education Agency, and Federal Education Initiatives.
- Any Use of the Whitehouse ISD Network for commercial and/or for-profit purposes is expressly prohibited.
- Extensive use of Whitehouse ISD Network for personal or private business is expressly prohibited.

- Users shall not seek information on, obtain copies of, and modify files, other data, or passwords belonging to other users on the network.
- All communications and information accessible via the Whitehouse ISD Network shall be assumed to be private property or the property of Whitehouse ISD.
- No use of the Whitehouse ISD Network shall serve to disrupt the use of the network by others; hardware and/or software shall not be destroyed, modified, or abused in any way. Vandalism is defined as any malicious attempt to harm or destroy data of another user.
- Malicious use of the Whitehouse ISD Network to develop programs that harass other users or infiltrate a computer or computing system and/or damage the software components of a computer or computing system is prohibited.
- Hate mail, harassment, discriminatory remarks, pornographic references or graphics, and other antisocial behaviors are prohibited on the Whitehouse ISD Network.
- The illegal installation of copyrighted software for use on District computers is prohibited
- Any violations of the use of Whitehouse ISD Network should be reported to the teacher, supervisor and/or technology director. You will be considered an accessory to the policy breach if you do not report seen violations.
- User will accept the responsibility of maintaining the integrity of the private electronic mail (e-mail) system. Users must report all violations of privacy or unacceptable contacts.
- User will notify Network Administrator if any virus is detected and from what apparent source.

All technology will be utilized for educational purposes (i.e. games without educational objectives are not permitted at **anytime** and may result in the loss of privileges to technology.) If games are used for educational objectives, those objectives and the selected games must be documented in the lesson plans.

Staff will be responsible for making sure that classroom substitute teachers are advised that students will not utilize computers unless specific written instructions have been left by the classroom teacher on proper/educational use of technology for **a specific class** period.

Failure to document use or failure to use technology for ethical and educational purposes **will** result in the reassignment or relocation of technology.

STUDENT SAFETY ISSUES

Maintaining student safety must be a priority for all. Safety issues involve the following: (PLEASE READ CAREFULLY!)

- Students' last names, phone numbers, addresses, or other personal information will not be utilized over any network without express permission from the student and the parent. Please help all your students understand how important it is for them to remain anonymous over the Internet. This is exactly the same precaution we use when a stranger calls our home.
- Students should not join any group of activities on the Internet that have not been recommended to them through the Texas Education Network or another legitimate educational resource.Students need to be informed that all network activity is monitored.
- Students should be encouraged to report any unethical behavior that they encounter while using any network, whether in e-mail or at any Internet site. This behavior includes cyberbullying. The FBI actively supports schools by the arrest and prosecution of those who participate in illegal activity on the Internet.
- Students must follow the guidelines given by teachers regarding online behavior and interacting with other individuals in chat rooms and social websites.

ETHICAL USE POLICY:

In compliance with the state of Texas, Whitehouse schools adhere to the ethical use of all technological tools, networks, and the Internet. Ethical Use is defined as the following:

Ethical Use of technologies refers to the utilization of resources, either hardware or software, in such a way as to maintain trustworthiness, respect, responsibility, fairness, caring, and citizenship -- the six pillars of ethical character.

The following guidelines should be used with district technology equipment:

DO NOT:

- Turn on a computer without using a surge protector (one per machine)
- Turn off computer while in Microsoft Windows
- Keep computer on if it is covered -- the heat buildup is dangerous!
- DO NOT LOAD any program files on your computer's root directory.
- Load any shareware program or other software not purchased by the district. Viruses are transmitted without this precaution.
- Bump a computer or "jar" it, move it or the table it is sitting on while it is running. Keep printers off the same table as your computer. Movement of your computer may cause hard drive failure.
- Set other electronic equipment near your computer (phones, stereos, radios, coffee cup warmers, etc.)

- Plug other electronic appliances into your surge protector. This causes small surges that eventually can damage your computer.
- Unplug your computer while it is running. Use the surge protector switch to turn off your computer before you unplug the surge protector from the wall.
- Allow students to perform administrative tasks on your computer (i.e. add programs, delete programs, perform upgrades or maintenance.)

DO:

- Monitor student computer activity
- Keep dust and liquids away from your computer

WHAT IS THE INTERNET?

The Internet is a vast global network linking millions of large and small computers all over the world. The Internet empowers individuals to communicate and collaborate with all types of agencies, research facilities, and academic resources around the world. Regardless of geographic location, the Internet provides users with a window to a world of information on almost any topic in the form of text, graphics, animation, sound, and video. The interactivity of the Internet assures students an active exchange of information that has never been possible before. Education has played an enormous role in development and use of the Internet. Scientists, researchers, writers, technicians, and investigators all contribute to the vast resources available to those who have access. Collaboration with students from around the world assist students in solving problems or identifying global warming trends, carcinogens, water contaminates, character development, technology infusion techniques, real-world solutions to energy crisis, and much, much, more.

USE OF INTERNET IN CLASSROOMS AND DISTRICT NETWORK:

In order for students to be able to use the Internet, the Acceptable Use Policy Contract must be read and accepted. This contract will include the parent, and student signatures. A student’s behavior and acceptable use of the Internet resources and school network will be directly monitored by the teacher.
Whitehouse ISD’s network has filtering for content in place. However, this filtering cannot be relied on to filter all content under all circumstances. Our network has protection against virus contamination and outside hacking, however, any unethical use of the network by students within the district will be a direct responsibility of the teacher. Any malicious behavior or unethical use of the networks will fall under the District Code of Conduct. Examples of misuse of Technology resources are:

- Violation of Copyright Laws.
- Misuse of equipment or defacing equipment.
- Unethical use of network, files, or Acceptable Use Policies.
- Accessing technologies for which one does not have permission to use (i.e. sharing a password, performing administrative tasks on a computer).
- Intentionally wasting limited resources, including the use of "chain letters", Chat Rooms, or broadcasting "SPAM" messages through mailing lists.
- Disruption of learning environment due to misuse of technologies.
- Referencing unauthorized technologies, files, or materials.
- Minor defacing or vandalism of technology.
- Minor damage to technology tools or resources.
- Insubordination or failure to comply with Acceptable Use Policies.
- Using technologies to do harm to an individual or to files or materials owned by others.
- Endangering another student or faculty member through revealing personal information (phone number, address, full name, etc.) over any network.
- Using technology to engage in threats or unethical activities (i.e. e-mail, or shared files).
- Using technologies without regard to human rights (such as forgery, vandalism, or password violations).
- Deliberately accessing files or resources that are not intended for student use.
- Using technology to engage in illegal acts or to solicit illegal activity.
- Using technology to engage in or imply lewdness.

- Violation of Copyright Laws that result in criminal offense.
- Deliberate destruction of district files, software, network equipment, or network resources.

WHITEHOUSE ISD'S TECHNOLOGY PLAN:

Whitehouse ISD's Technology Plan was accepted by the State of Texas and certified for three years. Our goals have been to:

- Provide Internet access to all rooms through the purchase of additional computers
- Add remote access to our network so that students & teachers may reach our district network from home
- Continue network infrastructure upgrades.
- Expand staff skills on network and Internet resources

EDUCATIONAL TECHNOLOGY PURCHASES

All state funded purchases for technology will be coordinated with the technology department, the district technology committee, campus principals and campus IMA committees..

EVALUATION OF TECHNOLOGY INFUSION:

Regular evaluation of technology infusion will be a part of Whitehouse ISD's Acceptable Use Policies and the PDAS. Teachers will maintain data (in lesson plans or grade book) to help faculty and administrators assess the success of technology infusion as related to achieving campus performance objectives.

FACULTY EXIT POLICY:

All teachers afforded technology by the district may be required to have an exit interview with a technology representative for discussion of equipment status. In the case of improper use, damage or loss, the employee may be held fiscally responsible.

STUDENT TECHNOLOGY ACCEPTABLE USE POLICY GUIDELINES:

Students of Whitehouse ISD will properly utilize technologies. Proper use includes real-world problem solving, independent and group productivity, research, design, and synthesis of ideas, and/or simulation exploration, experimentation, assessment and evaluation processes.
All students will understand basic and complex system design, maintenance, and acceptable use policies. Students wishing to utilize the district network and Internet resources will be required to have a teacher sponsor their access and each student must sign and have their parent's sign the Acceptable Use Contract.

All students will be required to follow ethical use, and copyright laws. Infringement of these policies will result in restriction or limited use of technology in Whitehouse ISD. Public domain software may not be uploaded or downloaded by a student without written permission from the director of technology.

Technology tools are provided by the district for appropriate educational objectives (i.e. games such as Solitaire, will not be played during school hours). Students utilizing technology for unauthorized purposes may be restricted from or lose privileges to district technologies.

The Technology Department will set the following disk space allocations for student directories:
High School – 1gb Junior High –500mb Holloway – 500mb
Higgins –250mb Brown – 250mb Cain – 250mb Stanton-Smith – 250mb

These space allocations are determined by teaching criteria, demand, campus size and server resources available.

Students will maintain equipment and report any equipment failure, damage or loss to their teacher. A student's failure to report important damage or loss may result in restricted use or loss of privileges to technologies.

Since technology equipment is district property, student violation or abuse of this equipment will be subject to disciplinary action as defined in the District Code of Conduct.

STAFF TECHNOLOGY ACCEPTABLE USE POLICY GUIDELINES:

All e-mail will be retained in accordance with local and federal retention policies on the Whitehouse Independent School District's Network. Attempts at forgery of electronic mail, password accounts, and files are expressly prohibited.

Staff home directories are monitored on an ad hoc basis and users are expected to maintain reasonable care in saving files with regards to space. If system resources begin to fill, individual limits will be put in place.

Since technology equipment is district property, violation or abuse of this equipment will be subject to disciplinary action.

Lab Policies

1. Schedule the use of the lab ahead of time.

2. As the facilitator, you should become familiar with what programs are available and what hardware is available in each lab and plan your activities accordingly.
3. Students MUST be accompanied by their teachers. Students are NOT to be sent to these labs without an accompanying teacher. This is part of Whitehouse's AUP.
4. Students should take pride in the facilities and leave the labs clean and neat.
5. Students are NOT to download anything (including cursors, screen savers, etc.) while they are in these labs, unless they receive permission from the teacher.
6. If you use the labs, you need to be aware of whether or not your students have their own network accounts. If they do not, then you should take a part of your research skills time to teach them about the AUP and have them apply for accounts. You should be sponsoring and training your own students.

Try to utilize these labs more often. As you know, research is a vital part of everyone's curriculum. We encourage you to teach your students proper research skills and habits before they come to the labs or during their time in the lab.

Please don't assume that they KNOW how to make efficient keyword searches or how to abide by copyright laws.

Section III:

Policies and Procedures for Users of District Owned Laptop Computer Equipment

The following has been provided to help assist our staff in obtaining information concerning questions they may have. If you have any questions concerning anything listed herein please feel free to contact us. We will be glad to answer any questions you may have.

Laptop Computer Use Agreement information

Due to the proliferation of portable devices such as Laptops, SmartPhones, Tablets, iPads, and other devices, the *Laptop Computer Use Agreement* has been eliminated. All approved district portable devices now fall under the support of Whitehouse ISD, and shall be subject to the same policies covered in Sections I and II of this document. This in no way limits your financial responsibility for lost, stolen or damage to equipment in your possession while off campus.