HHS & HMS Technology Handbook for Students

Hawkins ISD

Acceptable Use Policy for Students

The Purpose of the Acceptable Use Policy (AUP)

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

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

The Children's Internet Protection Act (CIPA) is a federal law enacted by Congress to address concerns about access to offensive content over the Internet on school and library computers. Hawkins ISD subscribes to Internet services through SuperNet. In accordance with CIPA, Hawkins ISD utilizes filtering & firewall tools in an effort to block objectionable materials from user access. Filtering software is not 100% effective; while filters make it more difficult for objectionable material to be received or accessed; filters are not a solution in themselves. Therefore, the rules and regulations in this document have been developed for the purpose of establishing acceptable and unacceptable use of the electronic communication systems and electronic resources within the district. CIPA guidelines are incorporated into this document as required by law.

Child Internet Safety Policy (CIPA) For Hawkins ISD in Compliance with FCC-11-125A1

Introduction

It is the Policy of Hawkins Independent School District to:

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

Definitions

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

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

Inappropriate Network Usage

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

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

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

Education, Supervision, and Monitoring

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

HISD Electronic Communications Systems

The use of network and electronic resources is a privilege, not a right. Inappropriate use may result in the cancellation of the privilege. Certain state and federal statutes may apply to the electronic communications system and inappropriate uses may also be unlawful. Unlawful use of district electronic resources will be referred to proper authorities. District authorities, under the rules of the appropriate campus handbook and the Student Code of Conduct, may also initiate other disciplinary actions.

Should a district user violate any of these provisions listed here, his or her account may be terminated, future access may be denied and disciplinary actions taken under the guidelines of the campus handbook and the Student Code of Conduct. In addition, all users are held responsible for understanding that the inappropriate use of the communication system may be a violation of state, federal, and local laws, including but not limited to: Section 1030 of Title 18 of the United States Code Fraud and Related Activity in Connection With Computers, as well as the Texas Computer Crimes Statute, Section 1, Chapter 33.02 of Title VII of the Texas Penal Code, Breach of Computer Security, and Section 16.04 of Title IV of the Texas Penal Code Unlawful Access of Stored Communications. Violations can lead to investigation and prosecution by law enforcement agencies.

Each user must attend training on appropriate use and Internet access, as well as sign a form acknowledging the rights and responsibilities of access to the electronic communications system. In those cases in which the user is under 18 years of age, the parent or legal guardian will be required to read and sign the Technology Handbook form.

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

The district's system is provided on an as is, as available basis. The district does not make any warranties, whether expressed or implied, including, without limitation, those of merchantability and fitness for a particular purpose with respect to any services provided by the system and any information or software contained therein. The district does not warrant the functions or services performed by, or the information or software contained on, the system will meet the system user's requirements, or the system will be uninterrupted or error-free or defects will be corrected.

Opinions, advice, services, and all other information expressed by system users, information providers, service providers, or other third party individuals in the system are those of the provider and not the district. The user is responsible and liable for any misuse of the system or system resources. The district will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the district's electronic equipment.

The district will provide training in the use of network resources. All users can download a copy of the Hawkins ISD Technology Handbook. All training in the use of the district's system will emphasize the ethical use of technology resources.

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

HB 2003 – Online Harassment

(See http://www.legis.state.tx.us/tlodocs/81R/billtext/html/HB02003F.htm for the entire HB)

Effective date: September 1, 2009

This bill creates the offense of online harassment. A person commits a third degree felony if the person uses the name of a another person to create a Web page on or to post one or more messages on a commercial networking site without obtaining the other person's consent and with the intent to harm, defraud, intimidate, or threaten any person.
A person also commits a class A misdemeanor 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 a person:

- Without obtaining the other person's consent;
- With the intent to cause the recipient of the communication to reasonably believe that the person authorized or transmitted the communication; and
- With the intent to harm or defraud any person.

This offense is a third degree felony if done with the intent to solicit the response of emergency personnel. It is a defense to prosecution that actor is acting on behalf of a commercial networking site, an Internet Service Provider, or other technology service provider.

Email

The district currently utilizes a student filtered email service. Not everyone will be issued an email account. The following rules are representative (but not inclusive) of how the email system is to be used as determined by the district.

Please note that email is not guaranteed to be private. District officials who operate the system do have access to all email. In addition to this, all email is subject to open records requests in accordance with the Public Information Act (a.k.a. Texas Open Records Act.) Monitoring of email by designated staff may occur on occasion to ensure appropriate use. **Messages relating to or in support of illegal activities will be reported to the authorities *(school, local, state, or federal).***

Student e-mail accounts, grades 7th-12th, will be assigned for the sole purpose of completing assignments as required by the classroom teacher. **The use of a student e-mail account must be in support of education and/or research as well as remain consistent with the educational objectives of the district.**

Students may only access district provided email accounts on district provided devices.

Chat Room use, blogging, and posting to a personal website that does not pertain to an educational goal assigned by a teacher while at school is not permitted .

Sending of Chain Letters or broadcast messages (spamming) to lists or individuals, and any other types of use, which may cause congestion of the networks or otherwise interfere with the work of others is prohibited. This includes forwarding junk mail to other users.

Transmission of information, which violates or infringes on the rights of any person or any abusive, profane, or sexually offensive information is prohibited. Emails of this nature, will be flagged by our filtering service, and reported to the campus Principal and Counselor.

Documents, images, unauthorized downloads, etc…will be removed from computers. Students are encouraged to back up any items he/she desires to keep. Students are encouraged to use Google and Google Docs to save items to. All student email accounts are disabled during the summer months and not available for use.

HISD Internet & Electronic Resources

The Internet is an electronic highway connecting millions of computers all over the world and millions of individual subscribers. Some of the major information sharing tools available via the Internet include:

- Electronic mail or email that allows communications with people all over the world. The network administrator or a designee will assign Email accounts.
- Instant Messaging (IM) and/or Text Messaging is the exchange of text messages through a software application in real time.
- File transfer protocol or FTP sites that have information of value to K-12 education.
- Blogs or personal online journal that is frequently updated and intended for general public consumption.

Through the use of the Internet, teachers, students, and staff have access to worldwide information resources. Through the utilization of district resources, faculty, staff, and students of the Hawkins Independent School District have the opportunity to create their information resources in a graphical environment.

The district's goal in providing these services is to promote educational excellence in the schools by facilitating resource sharing, innovation, and communication. Not all of the Internet capabilities listed above will be immediately available to faculty, students, and staff.

With access to computers and people all over the world comes the availability of materials that may not be considered of educational value in the context of the school setting. The district will strictly enforce rules that restrict access to objectionable material. However, on a global network, it is impossible to control all materials. The district believes that the valuable information available on the Internet far outweighs the possibility that users may see or access materials that are not consistent with the educational goals of the district.

Internet access is coordinated through a complex association of government agencies, and regional and state networks. In addition, the smooth operation of the network relies upon the proper conduct of the end users who must adhere to strict guidelines. These guidelines are specified here so each user is aware of the responsibilities he or she is about to undertake. Guidelines are considered the same as rules in this handbook.

The user is responsible and liable for any misuse of the system or system resources. The district will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the district's electronic equipment.

Consent

The district will provide all users with copies of the HISD Technology Handbook. All training in the use of the district's system will emphasize the ethical use. Students will be supervised at when using the district's computers and while accessing the Internet for educational purposes. Employees supervising the students will provide training to them emphasizing the appropriate ethical use of electronic resources and care of district equipment.

Availability of Access

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

- Imposes no tangible cost on the district
- Does not unduly burden the district's computer or network resources; and
- Has no adverse effect on a student's academic performance.

Community Use

Access to the district's electronic communication system including the Internet shall also be made available to members of the community, in accordance with administrative regulations. Such use may be permitted so long as the use:

- Imposes no tangible cost on the district
- Does not unduly burden the district's computer or network resources

Community members may utilize the Hawkins ISD wireless bandwidth after school hours from designated locations on the property. Community users are required to comply with all district rules, regulations, and policies governing appropriate use of the system. All users will be subject to filtering that is compliant with CIPA standards.

Internet Responsible Use

The following rules are representative (but not inclusive) of how the Internet is to be used as determined by the district. These bulleted rules apply for district owned computers at all times and for use of the network during school hours.

- Use of any other organization's network or computing resources must comply with the rules appropriate for that network.
- Use for commercial activities is prohibited including entering contests
- Use of the district network to purchase products is not permitted
- Use for product advertisement, including personal property, or political lobbying is prohibited

Users shall not use district computers or networks for any non-instructional or non-administrative purposes. This includes such programs as games or Multi-user Dungeons (MUDS), as well as video and audio streaming to the desktop. Continual connection to video and audio streaming can cause congestion on the district's network. Users are not to engage in this practice.

Access to specific resources such as IRCs (Internet Relay Chat) will be limited to activities in direct support of educational goals and only as authorized by the teacher for instructional purposes.

While software and shareware are available over the Internet, the quality of the software and impact on the system cannot be guaranteed. These programs may also contain viruses. Software, freeware, and shareware **shall not** be downloaded to individual user accounts or computers **without the express permission of the Technology Director**. The district will not be responsible for shareware downloading and fees. Shareware will not be supported by the technology department.

All communications and information accessible via the network are assumed to be the property of the publisher and/or sender and, as such are copyrighted. They cannot be distributed or copied without permission. This consideration is especially important for those who use e-mail and post messages to groups with an educational focus.

Netiquette (Network Etiquette)

Netiquette is a term describing the generally accepted rules of behavior on networked systems. District staff and students are expected to abide by these rules and will be revoked for violation of these rules.

.

- Be polite. Never be abusive to others.
- Use appropriate language. Do not swear, use vulgarities, or any other inappropriate language.
- Illegal activities are strictly prohibited.
- Never reveal personal addresses, and phone numbers or those of any other students, teachers, or staff members.
- Be brief. Few people will bother to read a long message.
- Minimize spelling errors. Be sure messages are easy to understand and read.
- Use accurate and descriptive subject titles for messages and articles.
- Cite references for any facts presented.
- Forgive the spelling and grammar errors of others
- Do not attempt to access teacher tools such as e-mail, grade book, or attendance. Students who access these programs will lose all computing privileges and be referred to campus principals for further disciplinary actions.
- Do not use the network in such a way as to disrupt the use of the network by other users.

Security

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

Using another individual's account and password is forbidden. Any user who allows another to use his/her account and password will lose his/her network privileges. Students are responsible for the protection of account passwords. Account names and passwords should not be shared with other individuals. If others are suspected of using another's account, notify the system administrator or teacher immediately.

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

Anyone illegally obtaining and using access to other computer systems may be the focus of state or federal investigation and prosecution. Applicable state statutes include Section 16.04, Unlawful Access to Stored Communications, and Section 33.03, Breach of Computer Security. If unacceptable or illegal activities take place while a user account is active, the account owner may be held responsible, regardless of whether that owner personally took the actions. Such activities may result in loss of access to computers and the Internet or other disciplinary actions.

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

Vandalism

Any malicious attempt to harm or destroy district equipment or materials, 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 will be viewed as violations of district policy and administrative regulations and possible criminal activity under applicable state and federal laws—this includes, but is not limited to the uploading or creation of computer viruses. Unauthorized technical work on district equipment will be considered vandalism. Vandals will lose computing privileges.

Disclaimer of Liability

The district shall not be liable for users' inappropriate use of electronic communication resources or violations of copyright restrictions or other laws, user's mistakes or negligence, and costs incurred by users. The district shall not be responsible for ensuring the accuracy, age appropriateness, or usability of any information found on the Internet.

Information/Data Storage

Users may be granted disk storage space on the file server to store school related work or files. However, disk space is limited and the system administrators reserve the right to set quotas for disk usage on the system. A user who exceeds his or her quota will be advised to delete files. Users may request additional file space from system administrators. After notice, a user who remains in non-compliance of disk space quotas will have his or her files removed by a site administrator. Additionally, site administrators may find it necessary to recover disk space and remove files. The administrator will attempt to notify the user if possible so the files can be moved to a medium outside the system.

Flash drives may be used to backup user files, however, these external personal devices will not be supported by the technology department. The district and technology department will not be responsible for lost data, and data lost cannot be retrieved. You must use these devices at your own risk.

Guidelines for Safe Use of Computer Resources at School

The possibility of encountering objectionable material does exist and the district is unable to completely prevent access to such material. Efforts are made on a regular basis to block such objectionable sites. However, if a student accesses a site with information that contains objectionable material, he or she is to exit from the site immediately and inform a teacher.

Using electronic information resources can be of great educational benefit and allow students to meet people from all over the world—ranging from scientists to students from other countries. Remember other Internet users cannot be seen. People may misrepresent themselves. HISD faculty and staff will take every precaution to supervise use in order to ensure that Internet access is an appropriate and positive educational experience.

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

- Respect the legal protection provided by copyright and license of programs and data.
- Respect the rights of others by complying with all district policies regarding intellectual property.
- Respect the rights of others by complying with all district policies regarding sexual, racial, or other forms of harassment, and by preserving the privacy of personal data.
- Respect the privacy of others by not tampering with their files, passwords, or accounts, or representing others when messaging or conferencing.

Many students will have the privilege of using laptops. Other students will have access to iPads, workstations in computer labs, the campus library, and in classrooms. For security purposes and confidentiality, students are not allowed to use computers designated for district employees, including teacher computers.

Use only computer IDs or accounts and communications facilities authorized for student use and use them for the purposes for which they were intended.

- Respect the integrity of computing systems and data. For example, do not intentionally develop programs (such as viruses) or make use of already existing programs that harass other users. Infiltrating a computer or computing system, and/or damaging or altering the software components of a computer or computing system, or gaining unauthorized access to other facilities accessible via the network is prohibited. **Additionally, personal computers/laptops or other computing devices such as tablets, iPads, etc… may not be utilized at school due to potential security issues, filtering requirements, computer viruses, and/or theft.** Personal jump drives or flash drives may be used at the user's own risk. Students are not to use MiFi hotspots. These devices, if detected on campus will be confiscated and returned to the parent only.

Copyright

Many people don't realize the legal ramifications of copyright violations. According to the Texas Association of School Boards, "the law no longer requires the owner of a work to put a "©" on it to give notice of the copyright, [therefore,] one should probably assume that use of anything on the internet or the World Wide Web is restricted unless the author gives notice that it's not." If uncertain about whether copyright rules apply, don't copy it.

The same can be said for information posted on district web pages. Individuals creating web pages must take extra precautions to prevent the inclusion of copyrighted materials without giving proper credit to the creator of the material. Copyright violators may lose technology privileges and, in accordance with the Student Handbook, other disciplinary actions may be taken.

Transmission of any material in violation of any federal or state regulation is prohibited. This includes but is not limited to: copyrighted material, threatening or obscene material or material protected by trade secret (a guiding factor in defining what is obscene may be what is appropriate in a school library setting. Librarians can provide further information. The most common sense policy is, when in doubt-don't!).

Copyright Do's and Don'ts

- Do think twice before copying a product. If uncertain about copyright issues, ask a teacher, campus librarian, or check with the technology director.
- Do copy personal work to insure that a backup copy of files and records is available.
- Do make use of electronic resources on the network always giving credit where credit is due.
- Don't load unauthorized software on any computer or on the network. Contact the technology director if unsure about the appropriateness of software. Campus principals along with the technology director will approve software titles. Unauthorized software will be removed and problems created by such software may not be supported and assistance may not be provided. In situations regarding the network, all technology privileges will be lost.
- Don't make illegal copies of software to share with friends or for home personal use. Most software publishers will allow an owner to make one backup copy to be used only if the original is damaged or destroyed. Additional copying and distribution of software is not permitted without the written permission of the publisher. Renting of school owned software is also prohibited. This type of illegal distribution or copying is called software piracy and is punishable by law even if financial profit is not involved.

Intellectual Property Rights

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

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

Web Publishing Guidelines

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

Web contacts are selected from each campus to assist with the creation and development of campus and organizational web pages. Web contacts will also be responsible for submitting potential web pages to the Webmaster. Not all web pages will be published.
Below are guidelines that will aide in the construction of all web pages posted on the District web server. These guidelines do not replace the Hawkins ISD Responsible Use Policy. The personal information of students may not be published on the District web pages without a signed release form or written statement. This information includes but is not limited to names, email addresses, photos, personal addresses, fax numbers, phones numbers, and personal beeper numbers.

I. The District has established a web site for the purpose of promoting positive information about Hawkins ISD. Additional pages will be made available to the following individuals and organizations:
    a. Teachers desiring to publicize their class projects and success stories
    b. Organizations whose purpose is to promote organizational information and positive student outcomes
    c. Students, under the direct instruction of a teacher, for the purpose of fulfilling a class assignment
    d. Alumni Association for the purpose of gathering information about HISD graduates and posting reunion notices

II. Campus, class, and organizational web pages:
    a. Web pages produced for campuses, classes, and organizations can present information about the specific school, class, or organization's activities and may not be published on off-site servers without approval from the Campus Principal.
    b. Principals are responsible for approving the content of their school based web pages and gathering staff release forms
    c. Teachers are responsible for the content of all student created web pages and for acquiring the appropriate parental/guardian signed release forms
    d. Organizational sponsors are responsible for the content of their organization's web page and for acquiring the appropriate parental/guardian signed release forms for students
    e. All web pages are subject to review at any given time and may be rejected if deemed inappropriate by the webmaster

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

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

HISD Laptop/electronic device Lending Guidelines

Student technology devices are being provided via bond funding. As such, the entire community has made an investment in Hawkins ISD students and their learning environment. This means that students and their families have a responsibility to take the utmost care of these devices, respecting the trust that the community has placed in its students.

Laptop use in high school requires internet access. If internet is not available, the laptop will not operate. Laptops/electronic devices issued for student use in grades 9-12 will remain the property of HISD for use by the students. In the event that a laptop is damaged beyond repair or warrants extensive repairs that were determined to be caused by negligence, the student will return the computer to the Tech Department and the student will be required to use the computers located in computer labs or library until damages are paid for. Fees will be assessed for any negligent damage.

*Parents may purchase device insurance from a third-party vendor to cover non-warrantied accidental damage. https://my.worthavegroup.com/hawkinsisdtx offers one option. This is a policy between the parent and the insurance company, not Hawkins ISD.

Student Agreement High School

- ❑ I will bring my HISD issued laptop/electronic device to school EVERY day that I am in attendance.
- ❑ I will not use the HISD issued laptop/electronic device for non-academic purposes (games, downloads, chat rooms, instant messaging, viewing websites not related to assignments, etc.)
- ❑ I will charge HISD issued laptop/electronic device battery daily and will NOT loan out the laptop, power adapter, cords, or software to other individuals, and know that I will be issued the same laptop each year.
- ❑ I will transport the laptop/electronic device in a safe manner. I will not remove any of the labels or stickers placed on the case by the school district.
- ❑ I will keep the HISD issued laptop/electronic device off the floor where it could be stepped on or tripped over. I will keep food and beverages away from the laptop since they may cause damage to the computer.
- ❑ I will not disassemble any part of my HISD issued laptop/electronic device or attempt any repairs. I will report problems or technical difficulties to my teacher and take the laptop to the Help Desk for support or repairs.
- ❑ I understand that regulations have been addressed in the student code of conduct and the HISD Technology Student Handbook to emphasize responsible use of digital resources, the Internet, Cyberbullying, and Social Networking and agree to abide by those regulations. I further understand that obscene language and/or suggestive materials are prohibited. If such items are found, I understand that my HISD issued laptop will be re-imaged and I could face disciplinary actions.
- ❑ I understand that my laptop/electronic device is subject to Internet filtering as required by law and that my use of the laptop/electronic device may be monitored at any time. I further understand that if I attempt to access inappropriate websites that I may lose access to the laptop/electronic device and other disciplinary actions may follow if warranted.
- ❑ I understand that my laptop/electronic device is subject to inspection at any time without notice and remains the property of the district.
- ❑ I understand that good behavior is expected and poor behavior may be grounds for removal of the laptop from my possession.
- ❑ I assume full responsibility of my Hawkins ISD issued laptop/electronic device.

- ❑ I understand that I must have parent permission to take a laptop/electronic device off of school property. I further understand that I am subject to disciplinary action and loss of laptop/electronic device privileges if I violate this rule.

By signing the STUDENT LAPTOP LENDING AGREEMENT, both the student and the parent/guardian agree to the above terms.

_____ _____

Student Signature Date

Student Agreement HMS

- ❑ All 7th and 8th grade classrooms will be issued classroom sets of laptops/electronic devices. Students are not allowed to take these devices home
- ❑ All 7th and 8th grade students web history, searches and student email will be filtered
- ❑ Students must notify the Technology department of any damages as soon as they occur
- ❑ Students understand that they are not to write on or adhere anything of any kind to the laptop/electronic devices
- ❑ Students understand that regulations have been addressed in the student code of conduct and the HISD Technology Student Handbook to emphasize responsible use of digital resources, the Internet, Cyberbullying, and Social Networking and agree to abide by those regulations. I further understand that obscene language and/or suggestive materials are prohibited. If such items are found, I understand that I could face disciplinary actions.

By signing the STUDENT/PARENT LAPTOP LENDING AGREEMENT, both the student and the parent/guardian agree to the above terms.

_____ _____

Parent/Guardian Signature Date

Parent Agreement for Students attending HHS

- ❑ I acknowledge that my student and I are to follow the expectations as presented in the Student/Parent Laptop Lending Agreement, and the technology guidelines outlined in the HISD Technology Handbook, as well as the rules of my child's campus. Furthermore, I understand that a violation of these lending guidelines could result in the student facing disciplinary action and/or removal of the laptop from the student's possession.
- ❑ I will be responsible for monitoring my student's use of the Internet when he/she is not at school.
- ❑ I acknowledge that fraudulent reporting of theft will be turned over to the police and insurance company for prosecution.
- ❑ I understand that I must see to it that my student immediately reports any damages or losses of equipment to the technology department and that I must submit the required fees, if the damage is not covered under warranty, before the laptop/electronic device will be returned to the student for continued use.
- □ I agree to immediately return the District laptop/electronic device and peripherals in good working condition upon request.

By signing the STUDENT/PARENT LAPTOP LENDING AGREEMENT, both the student and the parent/guardian agree to the above terms.

_____ _____

Parent/Guardian Signature Date

Check one of the following options for technology use:

_____ I want my child to take his/her device home.

_____I **do not** want my child take his/her device home.

Signature of parent or guardian _____

Home Address _____

Home telephone number _____ Date _____