

## **INSTRUCTIONAL SERVICES**

**Policy 6320**  
**(Regulation 6320)**  
**(Form 6320)**

### **Libraries, Media and Technology Services**

#### **Acceptable Use Policy: Electronic Access**

##### **Introduction**

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

##### **Statement of Purpose**

Technology is of the utmost importance at District schools. We take great pride in the functionality and reliability of our technology infrastructure. The purpose of this document is to alert the staff and users of the network to the Acceptable Use Policies of the Hallsville R-IV School District in matters of electronic access, use and theft.

##### **Authorized Users**

The District network is for the faculty, staff and students of the District only. Any other individual(s) requiring access to the network or use of a workstation should contact the Superintendent's/designee's office for prior approval. Any unauthorized usage of the District network could result in disciplinary action up to and including termination for faculty or expulsion from the District campus for unauthorized users.

All users (and parents/guardians if under age of 18) will be required to sign a Computer Access Agreement (Form 6320), stating that they will abide by the rules and guidelines of this policy. Parents/guardians will be given the option of denying Internet access and requesting alternative assignments not requiring direct Internet access.

##### **Internet – Acceptable Use**

Internet access is a large part of the District network. The Internet is an invaluable learning tool for all ages. It should be noted, however, that the District views Internet access as a privilege and access can be revoked at the discretion of the District for blatant misuse.

1. All use must be consistent with the educational mission and goals of the District.
2. The intent of the use policy is to make clear certain cases that are consistent with the educational objective of the District, not exhaustively enumerate all such possible uses.
3. The Superintendent/designee may at any time make determinations that particular uses are or are not consistent with the purpose of the District.

### **Access to Inappropriate Material**

To the extent practical, technology protection measures shall be used to block or filter Internet, or other forms of electronic communications, access to inappropriate information. Specifically, as required by the Children's Internet Protection Act, blocking shall 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 shall be taken to promote the safety and security of users of the District's online computer network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications. Specifically, as required by the Children's Internet Protection Act, prevention of inappropriate network usage includes: (a) unauthorized access, including so-called 'hacking,' and other unlawful activities; and (b) unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

It is all staff members' responsibility to educate students about appropriate online behavior, including interactions with other individuals on social networking sites/chat rooms, and cyber bullying awareness and response.

### **Supervision and Monitoring**

It shall be the responsibility of all District employees to supervise and monitor usage of the online computer network and access to the Internet in accordance with this policy and the Children's Internet protection Act. Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of the technology coordinator or designated representatives.

### **Modifications**

The Board is authorized to amend or revise this Acceptable Use Policy as deemed necessary and appropriate.

## **INSTRUCTIONAL SERVICES**

**Regulation 6320**  
**(Form 6320)**

### **Library, Media and Technology Services**

#### **Acceptable Use Policy: Electronic Access**

##### **Hours of Operation**

Normal hours of operation are 8 a.m.-5 p.m. Monday through Friday excluding weekends and holidays. However the District takes great pride in the availability of its technology resources and the network is generally available 6:00 a.m. to 11:30 p.m., seven (7) days a week for access. It should be noted that upgrades and maintenance are required to the network from time to time and these frequently occur after hours. In cases of network downtime, the faculty will be given electronic notification eight (8) hours prior to the downtime if possible. Special consideration may be accommodated if a user informs the Superintendent/designee prior to the downtime.

##### **Remote Access**

Staff remote access is provided to the District network via the use of dial-up or TCP/IP services over the Internet via a Citrix server. Software and installation instructions can be obtained from the Media Center Specialists. Again, the District views remote access as a privilege and violation of any policy guidelines could result in that privilege being revoked.

##### **Disclaimer**

Hallsville R-VI School District does not warrant that the functions of the network or workstations will meet any specific requirements of the users, or that it will be error-free or interrupted; nor shall it be liable for any direct, indirect, incidental or consequential damages (including lost data or information) sustained or incurred in connection with the use, operation or inability to use the system.

##### **Privacy Not Guaranteed**

The Superintendent/designee may review files and monitor all computer, e-mail and Internet activity to maintain system integrity and ensure that users are acting responsibly. The Superintendent/designee may remove programs or files from the computer system that are deemed obscene, threatening, pornographic or otherwise detract from the mission statement or objectives of the District.

The District shall use filtering, blocking or other technology to protect students and staff from accessing internet sites that contain visual depictions that are obscene, child pornography or harmful to minors. The District shall comply with the applicable provisions of the Children's Internet Protection Act (CIPA) and the Neighborhood Internet Protection Act (NCIPA).

## **Problem Reporting Procedure**

Users should report all problems with hardware or software to their appropriate Media Center Specialist. If the Media Center Specialist cannot resolve the problem, the Media Center Specialist will complete a Trouble Call Worksheet on the issue and a technician will be dispatched.

## **Network Logins**

All users, unless they have personal User IDs for the network, should log in to the system using the Workstation ID labeled on the front of the machine. If a user with a User ID logs in to a machine they should log out when leaving the computer unattended. Computer labs may be left in a logged in state, providing they have been logged in with the appropriate Workstation ID. Any problems which arise from a user's account are the responsibility of the account holder.

## **Passwords**

Users who have required passwords on their network or Internet accounts should not create passwords that can be easily obtained, such as license plate numbers; user's, spouse's, children's or pet's names; telephone numbers; user's street names or brand of user's automobile, etc. Neither should they place their passwords where they can be easily obtained, such as under mouse pads, keyboards, blotters, etc. Rather, users should create passwords not found in an English dictionary, and are encouraged to use mixed alphanumeric character passwords. In short, users should make it difficult for an individual to crack their password.

## **Software Registration**

All software installed on the District's network must be registered to the District and documented as such with the Superintendent/designee. Any registration forms should be turned into the Superintendent/designee for completion and mailing.

## **On-Line Encounters**

1. For safety reasons, students are prohibited from giving out personal information, such as their name, address, telephone numbers or photographs to anyone outside the District via chat rooms, e-mail, forums or any Internet site without the written approval of their parent/guardian.
2. Neither shall students agree to telephone or meet with someone they meet on-line or through e-mail without the direct accompaniment of a parent/guardian.

3. If a student feels uncomfortable with any suggestions by or conversations they have with a person they meet on-line or through e-mail, they should report it immediately to their parent/guardian or teacher.

### **Network Etiquette**

Users will be expected to abide by the generally accepted rules of network etiquette:

1. Be polite. Do not become abusive in your messages to others.
2. Use appropriate language. Do not swear, use vulgarities or any other inappropriate language.

### **Internet, Software and Hardware Usage – Prohibited Procedures**

In order to maintain the integrity of the computer systems, certain practices are expressly prohibited. Any user seeing a misuse of this system should report it to his/her appropriate Media Center Specialist.

1. Users are prohibited from using a computer or network for any unlawful purposes such as the illegal copying or installation of software or violation of copyright laws, or attempting to or obtaining unauthorized access to a network (hacking).
2. Users are prohibited from intentionally writing, copying or introducing any computer code designed to self-replicate, damage or otherwise hinder the performance of any computer's memory, file system or software. Such software is often called a bug, virus, worm, Trojan Horse or similar name.
3. Users are prohibited from deliberately using a computer to threaten, annoy or harass others with language, images or other media. Users shall not deliberately access or create any obscene or objectionable information, language or images.
4. Users are prohibited from tampering with or intentionally damaging the system, damaging information belonging to others, misusing system resources or allowing others to misuse system resources.
5. Users are prohibited from gaining unauthorized access to equipment or data resources.

6. Users are prohibited from taking home any technology equipment (hardware or software) without permission from the Superintendent/designee.
7. Users are prohibited from removing, replacing or adding or gaining access to any hardware components of the computer system including monitors, keyboards, mice, CPU's, internal CPU components, modems, printers, cables, spike bars, etc. without prior clearance from the Superintendent/designee.
8. Users are prohibited from scheduling maintenance by 3<sup>rd</sup> party service providers on said components without prior authorization from the Superintendent/designee.
9. Users are prohibited from using the external device (e.g. printers, speakers, zip drives) on any personal computer system except for those owned by the District without prior authorization from the Superintendent/designee.
10. Users are prohibited from powering said components in any unprotected wall outlet.
11. Users are prohibited from installing any software on the personal computer system without prior authorization of the Superintendent/designee.
12. Users are prohibited from modifying any software settings on the personal computer system that concerns the workstation components, network or peripheral equipment.
13. Users are prohibited from downloading or installing any software from the Internet without prior authorization.
14. Users are prohibited from accessing Internet sties that are not designed for learning purposes. Sites that are graphic in nature such as pornography, chat rooms, hacker sites, drug cultures or cult web sites are strictly forbidden.
15. Users are prohibited from copying any software or data files, except those created by the user or the user's e-mail account, onto another personal computer system without prior clearance from the Superintendent/designee.
16. Users are prohibited from erasing, renaming or making unusable another person's computer files, programs or disks (including those of the District.)
17. Users are prohibited from playing nonacademic games on personal computer systems or any network systems, unless under the direct supervision or curriculum of a staff member.

18. Users are prohibited from giving their passwords to students or other individuals.
19. Users are prohibited from trying to discover another user's password.
20. Users are prohibited from using another person's name, password or account to send or receive messages on the network.
21. Users are prohibited from unauthorized disclosure, use or dissemination of personal information regarding minors.
22. Users are prohibited from using District computers or networks for personal profit, any noninstructional, or nonadministrative purposes.

**Disciplinary Action**

Violation of any conditions of use described herein may be cause for disciplinary action, denial of access, suspension, expulsion or discharge. When or where applicable, law enforcement agencies may be involved. Any questions or issues regarding this Acceptable Use Policy should be directed to Hallsville R-IV Schools administration.

**Libraries, Media and Technology**

**Computer Access Agreement**

**COMPUTER ACCESS AGREEMENT**

I have read and agree to abide by the policies specified within the Acceptable Use Policy for Hallsville R-IV Schools (Policy and Regulation 6320). I understand that any violation of this policy can result in disciplinary action, denial of access, suspension, expulsion or discharge. Parents/guardians may be held accountable for their child's violations.

User's Full Name: \_\_\_\_\_ Student #: \_\_\_\_\_  
(Please Print)

User's Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Parent/Guardian Name: \_\_\_\_\_  
(If user is under 18 years of age) (Please Print)

Parent/Guardian Signature: \_\_\_\_\_ Date: \_\_\_\_\_