Houston County Board of Education

Monitoring:	Descriptor Term:	Descriptor Code:	Issued Date:
Review: Annually, in November	**Use of the Internet**	**4.406**	**06/09/25**
		Rescinds:	Issued: **11/11/02; 07/08/13; 08/08/22**

The Board supports the right of staff and students to have reasonable access to various information formats and believes that it is incumbent upon staff and students to use this privilege in an appropriate and responsible manner.

EMPLOYEES

Before any employee is allowed use of the district's internet or intranet access, the employee shall sign a written agreement, developed by the Director of Schools/Designee that sets out the terms and conditions of such use. Any employee who accesses the district's computer system for any purpose agrees to be bound by the terms of that agreement, even if no signed written agreement is on file.

The Director of Schools/Designee shall develop and implement procedures for appropriate internet use which shall address the following:

1. Development of the Network and Internet Use Agreement;

2. General rules and ethics of internet access;

3. Guidelines regarding appropriate instruction and oversight of student internet use;

4. A uniform signature block for use by all district employees; and

5. Prohibited and illegal activities including, but not limited to, the following:[1]
    - Sending or displaying offensive messages or pictures;
    - Using obscene language;
    - Harassing, insulting, defaming, or attacking others;
    - Damaging computers, computer systems, or computer networks;
    - Hacking or attempting unauthorized access to any computer;
    - Violation of copyright laws;
    - Trespassing in another's folders, work, or files;
    - Intentional misuse of resources;
    - Using another's password or other identifier (impersonation);
    - Using the network for commercial purposes; and
    - Buying or selling on the internet.

STUDENTS

The Director of Schools/Designee shall develop and implement procedures for appropriate internet use by students. Procedures shall address the following:

1. General rules and ethics of internet use; and

2. Prohibited or illegal activities including, but not limited to:[1]
    - Sending or displaying offensive messages or pictures;
    - Using obscene language;
    - Harassing, insulting, defaming, or attacking others;
    - Damaging computers, computer systems, or computer networks;
    - Hacking or attempting unauthorized access;
    - Violation of copyright laws;
    - Trespassing in another's folders, work, or files;
    - Intentional misuse of resources;
    - Using another's password or other identifier (impersonation);
    - Using the network for commercial purposes; and
    - Buying or selling on the internet.

INTERNET SAFETY MEASURES[2]

Internet safety measures shall be implemented that effectively address the following:

1. Limiting the content accessible by students using the internet access provided by the district to content that is age-appropriate;

2. Protecting the safety and security of students when they are using electronic mail, chat rooms, and other forms of direct electronic communications using internet access provided by the district;

3. Preventing unauthorized access, including "hacking" and other unlawful activities by students online;

4. Restricting students' access to materials harmful to them; and

5. Preventing students from using internet access provided by the district to access websites, web applications, or software that does not protect students against the disclosure, use, or dissemination of their personal information.

The Director of Schools/Designee shall establish a process to ensure the district's education technology is not used for purposes prohibited by law or for accessing sexually explicit materials. The process shall include, but not be limited to:

1. Utilizing technology that filters, blocks, or otherwise prevents internet access (for both students and adults) to material that is obscene or pornographic;[3]

2. Prohibiting and preventing a user from sending, receiving, viewing, or downloading materials that are deemed to be harmful to minors;[4]

3. Maintaining and securing a usage log; and

4. Monitoring online activities of students.[2]

The Board shall provide reasonable public notice of and at least one (1) public hearing or meeting to address and communicate its internet safety measures.[2]

A written parental consent shall be required prior to the student being granted access to electronic media involving district technological resources. The required permission/agreement form, which shall specify acceptable uses, rules of online behavior, access privileges, and penalties for policy/procedural violations, must be signed by the parent/guardian of minor students (those under 18 years of age) and also by the student. This document shall be executed each year and shall be valid only in the school year in which it was signed unless parent(s)/guardian(s) provide written notice that consent is withdrawn. In order to rescind the agreement, the student's parent/guardian (or the student who is at least 18 years old) must provide the Director of Schools/Designee with a written request.

Complaints alleging a violation of the internet safety measures shall be submitted the Director of Technology. All complaints shall be reviewed to determine how to appropriately respond.

EMAIL

Users with network access shall not utilize district resources to establish electronic mail accounts through third-party providers or any other nonstandard electronic mail system. All data including email communications stored or transmitted on school district computers shall be monitored. Employees/students have no expectation of privacy with regard to such data. Email correspondence may be a public record under the public records law and may be subject to public inspection.[5]

INTERNET SAFETY INSTRUCTION[6]

Students will be given appropriate instruction in internet safety as a part of any instruction utilizing computer resources. The Director of Schools/Designee shall provide adequate in-service instruction on internet safety. Parent(s)/guardian(s) and students will be provided with material to raise awareness of the dangers posed by the internet and ways in which the internet may be used safely.

SOCIAL NETWORKING

1. Students are prohibited from accessing social media platforms using district internet except when expressly authorized by a teacher for educational purposes.[7]

2. District staff who have a presence on social networking websites are prohibited from posting data, documents, photographs, or inappropriate information that is likely to create a material and substantial disruption of classroom activity.

3. District staff are prohibited from accessing personal social networking sites on school computers or during school hours except for legitimate instructional purposes.

4. The Board discourages district staff from socializing with students on social networking websites. The same relationship, exchange, interaction, information, or behavior that would be unacceptable in a non-technological medium is unacceptable when done through the use of technology.

VIOLATIONS

Violations of this policy or a corresponding administrative procedure shall be handled in accordance with the existing disciplinary procedures of the district.

VENDOR CONTRACTS[8]

Prior to entering into any contract for the provision of digital or online materials created or marketed for kindergarten through grade twelve (K-12), the district shall obtain an assurance that the vendor shall adhere to state law. This determination includes ensuring that the vendor filters, blocks, or otherwise prevents access to pornography or obscenity and verifying that the technology prevents a user from sending, receiving, viewing, or downloading materials that are harmful to minors.

Legal References

1. TCA 39-14-602
2. 47 USCA § 254 (h)(5)(A) – (C), 254(l); 47 CFR § 54.520(c)(1)(i); 20 USCA § 7131; Public Acts of 2025, Chapter No. 195
3. TCA 49-1-221(a)(1)(C)(i)
4. TCA 39-17-901; TCA 49-1-221(a)(1)(C)(ii)
5. TCA 10-7-512
6. TCA 49-1-221(a)(1)(E)
7. Public Acts of 2025, Chapter No. 195
8. TCA 49-1-221(c)

Cross References

Use of Email 1.805
Use of Artificial Intelligence Programs 4.214
School and System Websites 4.407
Controversial Materials 4.801
Student Publications 6.704