



STUDENT ACCEPTABLE USE AGREEMENT Technology Resources

The Hays Consolidated Independent School District provides technology resources to its students and staff for educational and administrative purposes. The goal in providing these resources is to promote educational excellence in the schools by facilitating resource sharing, innovation and communication with the support and supervision of parents, teachers, and support staff. The use of these technology resources is a privilege, not a right.

Proper behavior, as it relates to the use of computers, is no different than proper behavior in all other aspects of Hays CISD activities. All users are expected to use the computers and computer networks in a legal, responsible, ethical, and polite manner. This document is intended to clarify those expectations as they apply to computer and network usage and is consistent with the Administrative Procedures for Electronic Communication and Data Management and District Policy CQ (Local).

DEFINITION OF DISTRICT TECHNOLOGY RESOURCES

The District's computer systems and networks are any configuration of hardware and software. The systems and networks include all of the computer hardware, operating system software, application software, stored text, and data files. This includes electronic mail, local databases, externally accessed databases (such as the Internet), CD-ROM, optical media, clip art, digital images, digitized information, communications technologies, and new technologies as they become available. The District reserves the right to monitor all technology resource activity.

OWNERSHIP OF ELECTRONIC FILES

Electronic files created, sent, received, or stored on District Technology Resources owned, leased, administered, or otherwise under the custody and control of Hays CISD are the property of Hays CISD.

PRIVACY

Electronic files created, sent, received, or stored on District Technology Resources owned, leased, administered, or otherwise under the custody and control of Hays CISD are not private and may be accessed or monitored by Hays CISD Executive Director of Technology or designee at any time without knowledge of the user or owner.

DISTRICT TECHNOLOGY RESOURCES: STUDENT ACCEPTABLE USE AGREEMENT

1. System users must report any weaknesses in Hays CISD computer security, any incidents of possible misuse or violation of this agreement to the proper authorities by contacting the appropriate management. This security weakness should not be demonstrated to other users.
2. System users must not share their Hays CISD account(s), passwords, or similar information or devices used for identification and authorization purposes. The user is responsible for the proper use of the above information at all times.
3. Passwords should not be written down. If it must be written down, try to write it in a way that cannot be deciphered (such as using a hint) and store it securely in a safe, unlikely-to-be discovered location.
4. Attempting to log on or logging on to a computer or email system by using another's password is prohibited. Assisting others in violating this rule by sharing information or passwords is unacceptable.
5. Student use of the computers and computer network is allowed when granted permission and supervised by a staff member.
6. No participation in any chat room accessed on the Internet is permissible for students or employees unless special permission is arranged through the District Technology Executive Director or designee.
7. Non-educational online communication tools such as but not limited to blogs, wikis, etc. should not be accessed at school. Educational online communication tools may be accessed in compliance with the Internet Safety Guidelines located in the Student Code of Conduct.
8. Improper use of any computer or the network is prohibited. This includes the following:
 - Using racist, profane, pornographic, sexually oriented, or obscene language or materials
 - Using the network for political activity, financial gain, or commercial activity

- Attempting to harm or harming equipment, materials or data
 - Attempting to send or sending anonymous messages of any kind
 - Using the network to access inappropriate and / or harmful materials
 - Knowingly placing a computer virus on a computer or the network
 - Streaming media, such as radio, games, video, etc., for non-educational purposes
 - Using the network to provide addresses or other personal information that others may use inappropriately
 - Purposely engaging in activity that may: harass, threaten, defame, slander, libel, malign, or abuse another individual or group.
 - Using the network for illegal purposes, in support of illegal activities, or for any other activity prohibited by District policy or guidelines
 - Proxy sites - Attempting to bypass or bypassing, the filtering device by using sites such as but not limited to proxy sites on the District's electronic communications system
9. System users must not intentionally access, create, store or transmit material, which Hays CISD may deem to be offensive, indecent or obscene (other than in the course of academic research where this aspect of the research has the explicit approval of the Hays CISD official processes for dealing with academic ethical issues).
 10. Non-Hays CISD email accounts are not provided or supported by the Hays CISD Technology Department.
 11. System users are asked to delete outdated files on a regular basis.
 12. System users must not encrypt communications so as to avoid security review or monitoring by the system administrator.
 13. System users must not waste district electronic communication system resources for non educational purposes. (Distribution of video or photos, listening to web radio, etc.)
 14. Copyright: All users are expected to follow existing copyright laws, copies of which may be found in each campus library. Users must not make unauthorized copies of copyrighted software. **See District Copyright Guidelines – Student Code of Conduct.**
 15. Software applications may not be placed on any computer, whether stand-alone or networked to the District's system, without permission from the District Executive Director of Technology or designee.
 16. System users must not use non-standard shareware or freeware software without Hays CISD Technology designee approval.
 17. System users may not download any type of file sharing software without Hays CISD Technology designee approval.
 18. System users must not degrade the performance of District Technology Resources (ie. streaming video, streaming audio, and Internet radio); deprive an authorized Hays CISD user access to a Hays CISD resource; obtain extra resources beyond those allocated; circumvent Hays CISD computer security measures.
 19. System users must not download, install or run security programs or utilities that reveal or exploit weaknesses in the security of a system. For example, Hays CISD users must not run password cracking programs, packet sniffers, or port scanners or any other non-approved programs on Hays CISD District Technology Resources.
 20. System users must not plug unauthorized hardware into the Hays CISD network such as but not limited to wireless access points, personal laptop computers, or any non Hays CISD issued computer hardware.
 21. System users must not otherwise engage in acts against the aims and purposes of Hays CISD as specified in its governing documents or in rules, regulations and procedures adopted from time to time.

USER BACKUP

- The user is responsible for backing up data stored on their individual user network drive.
- Individual backups should occur at least once each six weeks during the school year.
- Backups should be placed on a secondary storage device such as a CD or USB memory stick.

VANDALISM PROHIBITED

Any malicious attempt to harm or destroy the District's equipment or materials, data of another user of the district's system, or any of the agencies or other networks to which the district has access, is prohibited. Deliberate attempts to degrade or disrupt system performance may be viewed as violation of District guidelines and possibly, as criminal activity under applicable state and federal laws, including the Texas Penal Code, Computer Crimes, Chapter 33. This includes, but is not limited to, the uploading or creating of computer viruses.

Vandalism as defined above will result in the cancellation of system use privileges and possible prosecution. The party will be responsible for restitution of costs associated with cleanup, system restoration, hardware, or software costs.

FORGERY PROHIBITED

Forgery or attempted forgery of electronic messages is prohibited. Attempts to read, delete, copy, or modify the electronic mail of other system users or deliberate interference with the ability of other system users to send/receive electronic mail is prohibited.

INFORMATION CONTENT/THIRD PARTY SUPPLIED 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 outside the District's networks that may contain inaccurate and/or objectionable material.

A student who gains access to such material is expected to discontinue the access as quickly as possible and to report the incident to the supervising teacher.

Hays CISD is making every effort to insure that the Internet environment is a safe one. HCISD is in compliance with the Children's Internet Protection Act (CIPA), which provides additional filtering for Internet security and safety. If you have questions or concerns regarding this policy, please contact the campus principal or technologist.

A student knowingly bringing prohibited materials into the school's electronic environment will be subject to suspension of access and/or revocation of privileges on the District's system and will be subject to disciplinary action in accordance with the Student Code of Conduct.

DISCIPLINARY ACTIONS

Hays CISD may suspend or revoke a system user's access to the District's system upon violation of this Acceptable Use Agreement or being identified as a security risk. Improper or unethical use may result in disciplinary actions consistent with the existing Student Code of Conduct or District policy. This may also require restitution for costs associated with system restoration, hardware or software.

Violation of this agreement may result in disciplinary action that may include suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of Hays CISD District Technology Resources access privileges, civil, and criminal prosecution.

NON-PARTICIPATION

Your child will have the opportunity and privilege to participate in approved online educational activities involving the Internet, including but not limited to, distance learning, podcasting, and online educational programs/subscriptions, unless you submit a letter to the school principal stating that your child is not to participate (please be specific).