



Student Acceptable Use Guidelines for Technology Resources

The purpose of this Acceptable Use Guidelines for Technology Resources is to ensure proper management of Harlandale's technology resources. For purposes of this document, “technology resources” can be defined as, but not limited to, electronic communication systems and electronic equipment. These resources include the District’s network, servers, computer workstations, laptops, mobile devices, peripherals, applications, databases, online resources, Internet access, e-mail, and any other technology designated for use by Harlandale ISD. Users are responsible for conducting themselves in an ethical and lawful manner. All network accounts maintained on Harlandale ISD systems are the sole property of the Harlandale Independent School District. The District may monitor all electronic communications and computer data and/or records. Use of the District’s technology resources including electronic communications and computers for commercial, religious, or political purposes is prohibited. The use of other user’s log-in credentials, attempting to access other user’s accounts without authorization, and modify other user’s electronic mail are prohibited.

The Internet is an electronic communications network that provides a resource for many types of communication and resources for diverse and unique information. It constitutes an unregulated collection of resources that change constantly. While the District uses filtering technology and protection measures to restrict access to inappropriate material, it is impossible to control all materials on a global network.

It is possible that you may run across some material you might find objectionable. In the same respect, e-mail received from outside sources cannot be fully controlled. SPAM, or unsolicited e-mail, is one of the single most widespread problems affecting technology resources and the Internet today. It will be each user’s responsibility to follow the rules for appropriate and acceptable use.

Harlandale ISD can monitor any user's e-mail account, as well as network accounts and computer drives, for legitimate reasons in accordance with this administrative regulation. Violation of this policy will result in disciplinary action and may result in termination or legal action.

Guidelines for Authorized Use

Harlandale's technology resources are intended primarily for educational use. As technology advances, the Internet has become a powerful information resource. Proper use of the Internet can enhance the capabilities of the individual and the district. In many cases, access to the Internet is becoming a job necessity. Because the Internet is an unregulated collection of resources that change constantly, organizations are responsible for placing the appropriate Internet usage restrictions upon their employees and students. This document explains the acceptable and unacceptable uses of the HISD technology resources.

The following are specific provisions regarding authorized use of the technology resources:

1. Use of the Internet is a privilege.
2. Users' online conduct must reflect the ethics, professionalism, courtesy, and responsibilities expected by HISD.
3. Data and files on the Internet must be considered copyrighted material and may not be distributed, copied, or published in any form without the written permission of the originator except as detailed in Title 17 of the United States Code, section 107, "Fair Use Doctrine". Users shall observe all provisions of copyright law in using material obtained from network sources. Federal law prohibits the transmission (sharing) of copyrighted materials without expressed written permission from the copyright holder. Copyrighted works include, but are not limited, to original writings, software, movies, and music. Material does not need to have a copyright on it to be protected under U.S. Copyright Law.
4. When account ID's and passwords for Internet services are entrusted to a user, the user becomes personally responsible for maintaining the integrity of the account. Network users are responsible for any network activity linked to their account. All passwords must be kept private. Much of the information on the HISD network is confidential and legally protected. To ensure unauthorized use of accounts, users should safeguard the security of the desktop when leaving the workspace.
5. Users must remember that data sent over the Internet should be considered "public" and readable by anyone. Special consideration should be taken before transmitting sensitive information. Consult with a supervisor if there is a question to the sensitivity of the material.
6. Workstations, laptops, and/or mobile devices are the responsibility of those they have been assigned to. Users must understand that it is their responsibility to secure those items assigned to them, as well as the data the devices contain. It is the user's responsibility to immediately contact their administrator and Information Services if any of the hardware, software, or data goes missing or is compromised.

The following are specific provisions regarding unauthorized use of district technology resources:

1. Users may not use technology resources for personal or financial gain or to support or oppose political candidates, groups, or ballot measures. Conducting union business without prior authority or consent of the superintendent is not allowed. Promoting, supporting, or celebrating religion or religious institution is restricted.
2. The use of abusive, vulgar or objectionable language on the Internet is unacceptable. Users will not use the system to access, upload, download, transmit or display or distribute obscene or sexually explicit material (pornography). Additionally, using the Internet for the intentional harassment or harm of an individual or organization or that advocates violence or discrimination towards other people (hate literature) is prohibited. It is not acceptable to use the district's networking services, resources or facilities for any purposes that violate existing state or federal laws, regulations, or District policies or procedures
3. Activities that compromise network security are strictly forbidden, including the disclosure of system ID's, passwords, or information that can allow the circumnavigation of security features. Users may not damage, delete, or destroy district files. Activities that disrupt or congest the district's network are forbidden. These include but are not limited to e-mail chain letters, unauthorized online games, music downloads, Internet file sharing (also called Peer-to-Peer Networks) and non-educational video broadcasts.

4. Network administrative software/tools such as network packet analyzers, network security discovery tools, and administrative applications are prohibited. Unauthorized networking equipment (including but not limited to: routers and wireless access points, tethering, mobile hot spots, etc.) is prohibited from use on the network. Network services and wiring may not be modified or extended beyond their intended use. Forgery or other misrepresentation of one's identity or use of another user's identity via electronic communication is prohibited regardless of intent.
5. All flash drives, CDs, and DVDs brought into the school or workplace from outside must be approved for use and scanned for viruses. The user will not knowingly run or install a program on any computer system or network or give to another user that intends to damage or to place excessive load on a computer system or network. Installation of software on district owned computers must be authorized and installed by Information Services. All software, all hardware (computers, devices, printers, document cameras, etc.) and all external services (including but not limited to cloud services, web hosting services, e-mail services, etc) must be submitted for technical compatibility review and pass that review by the Information Services Department before acquisition and use. No personal software, hardware or services will be installed on or accessed from HISD computers, devices or network.

The above list of prohibited actions is by way of an example only and is not intended to be exhaustive.

Privacy Issues

Users should not expect privacy in the contents of files or the record of Web research activities on the Harlandale ISD network. Routine maintenance and monitoring of the network traffic may lead to discovery that you have violated this guideline or the law. We reserve the right to inspect any and all files stored in all areas of our network in order to assure compliance with this policy. The District will cooperate fully with local, state, or federal officials in any investigation related to any suspected illegal activities conducted through the Harlandale ISD network.

When suspected violations of this Acceptable Usage Guidelines occur, appropriate Information Services department staff, the user's supervisor, and the Executive Director of Human Resources will be formally notified.

Acceptable Use Consent Form

I have read and understand the Harlandale Independent School District Acceptable Use Guidelines for Technology Resources and agree to abide by their provisions. I understand and allow the monitoring of my use of Harlandale's technology resources. I further understand and agree to retain electronic records, whether created or maintained using Harlandale's technology resources or using personal technology resources, in accordance with Harlandale's Record Management Program. In consideration for the privilege of using the Harlandale Independent School District's electronic communication system(s), and in consideration for having access to the public networks, I hereby release the Harlandale Independent School District, its operators, and any institutions with which they are affiliated from any and all claims and damages of any nature arising from my use of, or inability to use, the system, without limitation. I understand that Harlandale Independent School District will not be liable for my inappropriate use of technology resources, violations of copyright restrictions, or other laws, mistakes or negligence, and costs incurred. My access privileges may be revoked at any time with or without notice. I understand that inappropriate and prohibited use of the District's technology resources will result in disciplinary action and/or legal action against me.