

LIBERTY INDEPENDENT SCHOOL DISTRICT

ACCEPTABLE USE AND INTERNET SAFETY POLICY

Rev. 100208
Board Approved 3/9/2010

Introduction

This policy is applicable to all use of computing technology, network, and internet systems, herein referred to as the "System", while using school district property at any location or during school activities at any location. It applies to all System users including, but not limited to, students, faculty, employees, contractors, guests, and visitors.

The Superintendent or designee will oversee the System.

Network and Internet access is provided as an educational tool and is to be considered a privilege, not a right. The school district reserves the right to monitor, inspect, copy, review and store at any time and without prior notice any and all usage of the computer network and Internet access and any and all information transmitted or received in connection with such usage. All such information files shall be and remain the property of the school district and no user shall have any expectation of privacy regarding such materials.

All use of the System must be in support of education and research and be consistent with the mission of the district. In addition, educational technology may only be used in a manner consistent with federal and state law, license agreements and district policy. Commercial use of the District's system is strictly prohibited. Limited personal use of the system shall be permitted if the use:

1. Imposes no tangible cost on the District;
2. Does not unduly burden the District's computer or network resources; and
3. Has no adverse effect on an employee's job performance or on a student's academic performance.

System Access

System access is only allowed via login credentials, herein referred to as a "Login ID", assigned at the request of authorized district administrative personnel and created by employees of the LISD Technology Department (herein referred to as "Tech Department") or their designee.

The use of a Login ID constitutes agreement by the System user to abide by the information contained in this Acceptable Use Policy and to assume responsibility for all viewing, changes, access, and subsequent results associated with that account. The System user is responsible for their Login ID and should take all reasonable precautions to prevent others from being able to use the account. Under no conditions should a Login ID or password be provided to another person.

An "Access to Network Systems Agreement" form, herein referred to as "Agreement Form", must be signed and remain on file with the district for all System users. Some exceptions regarding the life of an Agreement Form exist for student System users and are noted in the section "Student Access Under Age 18" below.

Inappropriate Use and Internet Safety

Network and Internet access is a privilege which requires a high level of personal responsibility and may be denied due to inappropriate use.

Inappropriate use shall include but not be limited to:

1. Using the System for commercial purposes.
2. Using the System for personal purposes which:
 - a. Impose tangible cost on the District;
 - b. Unduly burdens the District's computer or network resources; and
 - c. Has an adverse effect on an employee's job performance or on a student's academic performance.
3. Using the System to transmit malicious information, rumors, or information known to be inaccurate.
4. Using the System to transmit ethnically or racially offensive language or slurs,
5. Using the System to transmit sexually oriented, or threatening materials or messages either public or private.
6. Using the System to bully, harass, demean, or otherwise harm any person or entity.

7. Posting private information about another person.
8. Using the System to send, receive, or view information regarding pornography, extreme violence, obscenities, nudity, drugs or other substances prohibited on school grounds, weapons, or otherwise objectionable material.
9. Engaging in any illegal act, such as arranging for a drug sale or the purchase of alcohol, engaging in criminal gang activity, threatening the safety of person, etc.
10. Damaging the security of the System.
11. Using another individual's Login ID or password.
12. Participating in computer "hacking" activities of any form.
13. Forging or attempting to forge electronic mail messages.
14. Attempting to read, delete, copy or modify electronic mail of other System users.
15. Attempting to disrupt the System or destroy data by spreading computer viruses.
16. Vandalizing the System.
17. Violating copyright laws.
18. Failing to follow network etiquette procedures.
19. Submitting false or misleading information to obtain or retain access to the System.
20. Accessing the System in any manner inconsistent with the mission of the school district.
21. Interfering with official school district communications.

Improper or unethical use may result in revocation of a user's Login ID and cessation of System access, disciplinary actions consistent with the district policy and, if appropriate, the Texas Penal Code or other state and federal laws. This may also require restitution for costs associated with system restoration, hardware, or software costs (also see the section entitled "Discipline" below).

Network Etiquette

System users are expected to observe the following network etiquette (also known as netiquette):

- Be polite. For example, messages typed in capital letters are the computer equivalent of shouting and are considered rude.
- Use appropriate language. No swearing, vulgarities, suggestive, obscene, belligerent, threatening language, or language which may be offensive to others.
- Be respectful of others' opinions.
- Don't assume that a sender of e-mail is giving his or her permission for you to forward or distribute the message to third parties or to give his/her e-mail address to third parties. This should only be done with permission or when you know that the individual would have no objection.
- Be considerate when sending attachments with e-mail (where this is permitted). Be sure that the file is not too large to be accommodated by the recipient's system and is in a format which the recipient can open.

Inappropriate Access to Material

As required by federal CIPA regulations, the System is equipped with an internet content filter. The System user will make no attempts to bypass the filter or access material that is denied by the filter unless authorized by the filter's "Override" feature.

If access to inappropriate material mistakenly occurs for a:

- Student - Immediately report it to a teacher, Principal, or Assistant Principal;
- Other - Immediately report it to the Principal or Assistant Principal, AND to the Tech Department.

This will help protect you against a claim that you have intentionally violated this Policy.

Student Access and Internet Safety

Students under the age of 18 must have the written approval of a parent or guardian before being allowed System access as indicated by a signed Agreement Form. Student privileges will be granted only for **one academic year**. A signature on the Agreement Form indicates that the person signing the form has read, understood, and agrees to information contained on the form and any supplemental information which may be provided with the form.

Students will have access to the System for class assignments and research with their teacher's permission and supervision.

Personal information such as addresses and telephone numbers will remain confidential when communicating on the system. Students will never reveal such information without permission from their teacher, LISD adult, parent, or guardian.

Students will never make appointments to meet people in person that they have contacted on the internet via the System without district and parent permission.

Security and Usage Guidelines

Under no circumstances will a System user login to a computing device (e.g. desktop, laptop, or netbook computer, or ANY other device which connects with to System) and then leave that computing device out of their sight while remaining logged in. All System users MUST either **completely log out** of the computing device or initiate a (much faster) "**system lock**" procedure prior to leaving that computing device out of sight. The System user may request assistance from a campus administrator, teacher, or the Tech Department if they do not know the proper "system lock" procedure.

System users will not seek information on, obtain copies of, or modify files, other data, or the Login ID belonging to other System users, or misrepresent other System users, or attempt to gain unauthorized access to the System.

Communications may not be encrypted so as to avoid security review.

A System user guide will be published and available for viewing and distribution via the internet or from any campus or administrative office. District employees will provide assistance to view the user guide if necessary.

All System users are responsible and compelled to notify a Tech Department employee or campus administrator promptly upon discovery of any suspected security breach.

The district reserves the right to remove a Login ID from the System or to disconnect any System user to prevent unauthorized activity or inappropriate use at any time.

Network and Internet access is provided as an educational tool and is to be considered a privilege, not a right. The school district reserves the right to monitor, inspect, copy, review and store at any time and without prior notice any and all usage of the computer network and Internet access and any and all information transmitted or received in connection with such usage. All such information files shall be and remain the property of the school district and no user shall have any expectation of privacy regarding such materials.

Copyright

System users may not illegally download or capture music, mp3 files, movies, books, stories, poetry, or any other copyrighted works.

System users may download material for their own use in accordance with applicable copyright laws, district policy and administrative regulations. The Fair Use doctrine allows an individual to reproduce portions of copyrighted work for non-commercial purposes, in some instances. Reproduction beyond fair use requires the permission of the copyright holder or authorized person. The permission must be specified in the document or must be obtained directly from the author in accordance with applicable copyright laws, district policy and administrative regulations. Violations of copyright law could lead to civil liability with excessive penalties.

The System user will not plagiarize works found on the Internet. **Plagiarism** is taking the ideas or writings of others and presenting them as if they were your own. **Copyright infringement** occurs when a person inappropriately reproduces a work that is protected by a copyright. If a work contains language that specifies appropriate use of that work, the System user should follow the expressed requirements. If the System user is unsure whether or not they can use a work, then they should request permission from the copyright owner.

Liability

The district does not warrant that the functions and services performed by or the information or software contained in the educational technology resources will meet the System user's requirements or that the system will be uninterrupted or error-free, or that defects will be corrected. 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 content or services provided by the System and any information or software contained therein.

The Agreement Form shall include a provision that the System user, parents or guardians (if applicable), will hold the district harmless from user violations of copyright laws, software licensing requirements, access of inappropriate materials, violations by the user of others' rights to confidentiality, free speech and privacy, and damage to internal and external systems accessed by the System user.

Updates

If, after the user signs an Agreement Form, some of the user's information changes, the user must notify the campus and/or district personnel of such changes and complete a new Agreement Form.

Also, a new Agreement Form may periodically be required to reflect changes in the law or technology. Such information must be provided if the user wishes to continue to use the System.

Discipline

A user who violates this policy, shall at a minimum, have his or her access to the System terminated, which the district may refuse to reinstate for the remainder of the user's association with the school district.

A user violates this policy by his or her own action or by failing to report any violations by other users that come to the attention of the user. Further, a user violates this policy if he or she permits another to use his or her Login ID or password to access the System, including any user whose access has been denied or terminated.

The school district may also take other disciplinary action in such circumstances.
Violations which may be criminal will be referred to appropriate law enforcement officials.