

Network Access General Use Policy for Employees

Guidelines for Acceptable Use of Lewisville Independent School District Technology Resources

The Lewisville 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 District's 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.

With access to computers and people all over the world comes the potential availability of material that may not be considered to be of educational value in the context of the school setting. Lewisville ISD firmly believes that the value of information, interaction, and research capabilities available outweighs the possibility that users may obtain material that is not consistent with the educational goals of the district.

Proper behavior, as it relates to the use of computers, is no different than proper behavior in all other aspects of Lewisville ISD activities. All users are expected to use the computers and computer networks in a 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 District Policy.

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), CDROM, optical media, clip art, digital images, digitized information, telecommunications devices, and all new technologies as they become available. The District reserves the right to monitor all technology resource activity.

ACCEPTABLE USE

The District's technology resources will be used only for learning, teaching and administrative purposes consistent with the District's mission and goals. Commercial use of the District's system is strictly prohibited.

The District will make training available to all users in the proper use of the system and will make copies of acceptable use guidelines available to all users. All training in the use of the District's system will emphasize the ethical use of this resource.

Software or external data may not be placed on any computer, whether standalone or networked to the District's system, without permission from the Executive Director of Technology or designee.

Other issues applicable to acceptable use are:

1. **Copyright:** All users are expected to follow existing copyright laws, copies of which may be found in each campus library as well as <http://www.lisd.net/librarysvcs/copyright.htm>.
2. **Supervision and permission:** A staff member only allows student use of the computers and computer network when supervised or granted permission.
3. **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.
4. **Improper use of any computer or the network is prohibited.** This includes the following:
 - Submitting, publishing or displaying any defamatory, inaccurate, racially offensive, abusive, obscene, profane, sexually oriented, or threatening materials or messages either public or private
 - Using the network for financial gain, political or commercial activity
 - Attempting to or harming equipment, materials or data
 - Attempting to or sending anonymous messages of any kind
 - Using the network to access inappropriate material
 - Knowingly placing a computer virus on a computer or the network
 - Using the network to provide addresses or other personal information that others may use inappropriately
 - Accessing of information resources, files and documents of another user without authorization

5. ***Inappropriate use of district computers to post blogs, forums or podcasts is prohibited.*** This includes the following:

Podcasts:

- Posting any student or teacher created Podcast projects that are not directly related to and in support of the LISD approved Curriculum.
- Posting any student or teacher created Podcast to the campus server.

**For additional information see the LISD District Podcasting Procedures document.

Blogs, Forums and Wikis:

- Posting any student or teacher created blog projects that are not directly related to and in support of the LISD approved Curriculum.
- Posting any student or teacher created blog to the campus server or external sites. Any such posting will be removed.
- Posting of any unsupervised student blog.

**For additional information see the LISD District Blog/Forum Procedures document.

SYSTEM ACCESS

Access to the District's network systems will be governed as follows:

1. Students will have access to the District's resources for class assignments and research with their teacher's permission. Teachers with accounts will be required to maintain password confidentiality by not sharing the password with anyone.
2. With the approval of the immediate supervisor, district employees will be granted access to the District's system.
3. Any system user identified as a security risk or having violated District Acceptable Use Guidelines may be denied access to the District's system. Other consequences may also be assigned.
4. Any system user having been denied access rights may be reinstated with a limited access account to reduce the level of security risk to the system. Limits on this type of account may include time limitations, station access limitations, file access restrictions, and a revocation of Internet access privileges.

CAMPUS LEVEL RESPONSIBILITIES

The campus principal or designee will:

1. Be responsible for disseminating, collecting signed permission forms, and enforcing the District Acceptable Use Guidelines for the District's system at the campus level.
2. Ensure that employees supervising students who use the District's systems provide information emphasizing the appropriate and ethical use of this resource.
3. Ensure that proper procedures are followed in requesting and acquiring all new or additional hardware or software.

INDIVIDUAL USER RESPONSIBILITIES

The following standards will apply to all users of the District's technology resources.

1. The individual in whose name a system account is issued will be responsible at all times for its proper use.
2. The system may not be used for illegal purposes, in support of illegal activities, or for any other activity prohibited by district guidelines.
3. System users may not use another person's system account.
4. System users are asked to maintain electronic mail or outdated files on a regular basis.
5. System users will be responsible for the care and maintenance of their systems. Maintenance issues should be reported to the campus computer facilitator.
6. System users will be responsible for following all copyright laws.
7. Users will be responsible for adhering to the LISD District Password Procedures.

VANDALISM PROHIBITED

Any attempt to harm or destroy District 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. Intentional attempts to degrade or disrupt system performance may be viewed as violations 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, system break-in utilities such as Sub7 or system hacking programs.

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 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 inadvertently provide access to other electronic communications systems outside the District's networks that may contain inaccurate and/or objectionable material. The District will maintain an Internet filtering software package to attempt to minimize the access to objectionable material. Any attempt to circumvent the filtering software will be viewed as an attempt to disrupt the system.

A student bringing prohibited materials into the school's electronic environment will be subject to a suspension and/or a revocation of privileges on the District's system and will be subject to disciplinary action in accordance with the Student Code of Conduct. An employee knowingly bringing prohibited materials into the school's electronic environment will be subject to disciplinary action in accordance with District policies. This could result in loss of credit for students or termination of employment for employees.

NETWORK ETIQUETTE

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

1. Use appropriate language: swearing, vulgarity, ethnic or racial slurs, and any other inflammatory language is prohibited.
2. Pretending to be someone else when sending or receiving messages is prohibited.
3. Submitting, publishing or displaying any defamatory, inaccurate, racially offensive, abusive, obscene, profane, sexually oriented, or threatening materials or messages either public or private.
4. Revealing such personal information as addresses or phone numbers of users or others is prohibited.
5. Using the network in such a way that would disrupt the use of the network by other users is prohibited.
6. Be polite. For example, messages typed in capital letters are the computer equivalent of shouting and are considered rude.

SUSPENSION/REVOCAION OF SYSTEM USER ACCOUNT

The District will suspend or revoke a system user's access to the District's system upon violation of District policy and/or administrative regulations regarding acceptable use.

Termination of an employee's account or of a student's access will be effective on the date the principal or campus coordinator receives notice of user withdrawal or of revocation of system privileges, or on a future date if so specified in the notice.

CONSEQUENCES OF IMPROPER USE

Improper or unethical use may result in disciplinary actions consistent with the existing Student Discipline Policy and, if appropriate, the Texas Penal Code, Computer Crimes, Chapter 33, or other state and federal laws. This may also require restitution for costs associated with system restoration, hardware, or software costs.

DISCLAIMER

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 fitness for a particular purpose with respect to any services provided by the system and any information or software contained therein. The District uses a variety of vendor supplied hardware and software. Therefore, the District does not warrant that the functions or services performed by, or that the information or software contained on the system will meet the user's requirements. Neither does the District warrant that the system will be uninterrupted or error-free, nor that defects will be corrected.

Opinions, advice, services, and all other information expressed by system users, information providers, service providers, or other third party individuals in the system are those of the providers and not necessarily the District.

The District will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the District's computer systems and networks.

TERM

This policy is binding for the duration of the current school year in Lewisville ISD. Electronic Mail and Additional Technology Guidelines for District Staff

Email has become one of the most used communications tools in both our constituents' homes and their work places. Email is an integral part of all LEWISVILLE INDEPENDENT SCHOOL DISTRICT classroom and offices, the following points are important and must be followed:

1. Electronic mail is a privilege not a right. All electronic communication is governed by the Network Access General Use Policy. All terms that are covered in the Network Access General Use Policy, including user responsibilities and consequences for policy violations, apply to Email.
2. The software and hardware that provides us email capabilities has been publicly funded. For that reason, it should not be considered a private, personal form of communication. The contents of any communication of this type are governed by the Network Access General Use Policy.
3. Blanket emails (those to all users in the district), must have authorization from Technology. All blanket emails must include as the first line "DO NOT FORWARD THIS EMAIL". This type email has the propensity to bring down the network due to the volume of traffic it creates.
4. Incoming email that is misaddressed will remain "undeliverable". Please be certain that you give out your correct email address. All Internet pages containing lists of staff addresses should also contain a disclaimer.
5. Requests for personal information on students or staff members should not be honored via email. It is critical for a personal contact to be made with any individual requesting personal information. In addition, security information such as username or password should not be sent via email for any reason.
6. No request for student grades, discipline, attendance or related information can be communicated via electronic mail unless a signed Release of Student Records is on file on the campus.
7. During student contact time in the classroom, staff members should not use email. Instant messenger programs or chat programs should not be active during class time.
8. Staff members should set aside time at least once a day to check, respond to, and maintain email messages.
9. Emails sent with the intent of advertising or selling any item, product or service (whether personal or for a business) would be considered commercial and is not permitted. See CQ (LOCAL) on LIMITED PERSONAL USE, item number 4.
10. Since email access is provided for school business related use, please do not forward messages that have no educational or professional value. An example would be any number of messages that show a cute text pattern or follow a "chain letter" concept. These messages should be deleted and the sender notified that messages of that nature are not appropriate to receive on your district email account.
11. Attachments to email messages should include only data files. At no time should program files (typically labeled ". Exe") be attached due to software licensing requirements. In addition, there exists the real possibility that any program files received as attachments over the Internet may include viruses or other very destructive capabilities once they're "launched" or started. If you receive an attachment like this, please delete the email message immediately without saving or looking at the attachment.
12. Subscriptions to an Internet listserv should be limited to professional digests due to the amount of email traffic generated by general subscriptions. Please use your personal Internet account to receive listserv subscriptions of a general nature, if one is available.
13. Students will not be issued individual email accounts. For any projects that involve email communications, use either your district account as a facilitator to the activity, or, work with your campus computer facilitator to activate a special project account for a limited time.
14. Please notify your campus technology facilitator if you receive unsolicited email, particularly if it is of a "hate mail" nature. The Technology department will attempt to track down the source of that email and prevent you from receiving any additional unsolicited mail.

User security responsibilities

1. Your username and password should be protected from unauthorized use at all time. Do not post any of this information where others can view it.
2. Do not share your password via email at any time. If a technology representative needs that information, they must request it in person.

Telecommunication Technology Guidelines for District Staff

1. The use of all district provided telecommunication equipment to include but not limited to desk phones, cell phones, Blackberries, Pagers, Walkie-Talkies, is a privilege not a right. All communication is governed by the Network Access General Use Policy. All terms that are covered in the Network Access General Use Policy, including user responsibilities and consequences for policy violations, apply to use of these devices.
2. These technologies have been publicly funded. For that reason, they should not be considered a private, personal form of communication. Personal use is inappropriate. The contents of any communication of this type are governed by the Network Access General Use Policy.

Maintenance of Local Hard Drives

All classroom teacher computers and some administrative computers allow access to the local hard drive for installing software. This access does not mean that personal software should be installed on district computers. On occasion hard drives need to be reformatted, (which completely erases all contents of the drive). A technology department technician will reinstall all productivity software that is purchased through the technology department. The technology department will not reinstall personal software nor will they retrieve personal data files. Please keep any installation disks for preview software or specific school-purchased software in an identified location at your campus should the need for reinstallation arise. You are personally responsible for making backups of any data files that are stored on your local hard drive.

1. All computers and video hardware are to be shut down each evening. This includes CPUs, monitors and VCRs.

Computer Software

The current configuration on district computers does not allow unauthorized software installation. Unauthorized software installation may affect network and machine performance adversely and is prohibited by the Guidelines for Acceptable Use of Lewisville Independent School District Technology Resources.

To ensure that software will not affect the current network configuration adversely, the following guidelines apply when you want to purchase software not listed in the technology catalog.

1. Contact the technology department to determine if another campus has purchased and installed the program. This will prevent repeated orders of programs that have been determined unsuitable for our network environment. All network software must be approved by the technology department and the curriculum supervisor responsible for the subject area, prior to purchase.
2. The Technology Department must be consulted prior to any purchase of software.
3. All software purchases must be purchased through and delivered to the technology department for installation.
4. To purchase new software, send a program specification sheet to the technology department as well as a description of the computers on which the program will be used.
5. Prior to installation on any campus, the campus computer facilitator must be consulted.

If a software program is determined to be unsuitable for the network it will not be installed. The campus will need to make arrangements to return the software for a refund, or replacement with standalone equivalents.

Our goal is to promote the use of appropriate, innovative software whenever possible. These guidelines will insure that the required support and installation process is in place before funds are expended.

Software will be installed only when there is documentation showing that the software purchase has gone through the process referenced above and that proper licensing has been purchased. Software purchased by staff using personal funds will be subject to all district guidelines. The documentation and license must be provided to the technology department or the campus computer facilitator prior to the installation of any personal software.

Computer Hardware

All hardware purchases should be for those items listed in the current technology bid since we have maintenance agreements on those items. For items not listed in the technology catalog, please work with the district technology purchasing agent.

1. Absolutely no one except approved vendors, district technicians, and certified computer facilitators are authorized to install computer hardware on any district equipment.
2. Campus computer facilitators may install hardware on campus systems if they have hardware certification through the technology department.
3. Hardware must be purchased through the Technology Department using the current technology bid or with approval by the technology purchasing agent.
4. All hardware must be purchased through and shipped to the technology department with documentation listing campus name and contact.
5. Campus computer systems may not be modified, upgraded, or replaced with donated equipment without the prior approval of the technology department.
6. To maintain accurate physical inventory campus computer systems are not to be moved from one room to another room on the same campus without the prior approval of the campus technology facilitator.
7. Campus technology systems may not be moved from one campus to another campus without the prior approval of the technology department.

This page intentionally left
blank

Employee agreement for acceptable use of the electronic communications system

You are being given access to the District's electronic communications system. Through this system, you will be able to communicate with other schools, colleges, organizations, and people around the world through the Internet and other electronic information systems/networks. You will have access to hundreds of databases, libraries, and computer services all over the world. With this opportunity comes responsibility. It is important that you read the Guidelines for Acceptable Use of Lewisville Independent School District Technology Resources, and the agreement form.

Inappropriate system use will result in the loss of the privilege to use this educational and administrative tool. Please note that the Internet is a network of many types of communication and information networks. It is possible that you may run across some material that you find objectionable. While the District will use filtering technology to restrict access to such material, it is not possible to absolutely prevent such access. It will be your responsibility to follow the rules for appropriate use.

RULES FOR APPROPRIATE USE:

1. The account is to be used only for educational and administrative purposes
2. You will be held responsible at all times for the proper use of your account, and the District may suspend or revoke your access if you violate the rules.

INAPPROPRIATE USES:

1. Using the system for any illegal purpose
2. Using the system for advertising or selling any item, product or service (whether personal or for a business)
3. Disabling or attempting to disable any Internet filtering device
4. Encrypting communications to avoid security review
5. Borrowing someone's account without their permission
6. Downloading or using copyrighted information without permission from the copyright holder
7. Intentionally introducing a virus to the computer system
8. Posting messages or accessing materials that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal
9. Wasting school resources through the improper use of the computer system
10. Gaining unauthorized access to restricted information or resources

CONSEQUENCES FOR INAPPROPRIATE USE:

1. Suspension of access to the system
2. Revocation of the computer system account; or
3. Other disciplinary or legal action, in accordance with the District policies and applicable laws.

EMPLOYEE AGREEMENT:

I understand that my computer use is not private and that the District will monitor my activity on the computer system. I have read the Guidelines for Acceptable Use of Lewisville Independent School District Technology Resources and agree to abide by their provisions. In consideration for the privilege of using the District's electronic communications system and in consideration for having access to the public networks, I hereby release the 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, including, without limitation, the type of damages identified in the District's policy and administrative regulations.

I realize that I am responsible for the monitoring of network use by students under my supervision. I will immediately report any violations of the Network Access Policy to the campus principal.

_____ Employee Name -- (Please print)	_____ Employee Signature
_____ Home address	_____ Home phone number
_____ Date	
This space reserved for system administrator.	
_____ Assigned username	_____ Date