

NETWORK ACCESS GENERAL USE POLICY FOR EMPLOYEES



Table of Contents

Introduction	1
Consequences of improper use	1
Disclaimer	1
Electricity (clean power).....	2
Electronic Mail.....	2
Forgery Prohibited	3
Individual User Responsibilities	3
Information Content/Third Party Supplied Information.....	3
Information Systems Department Staff	4
Internet Access.....	4
Internet Usage	4
Maintenance of Local Hard Drives.....	4
Network Security	4
Network Etiquette	5
New Equipment	5
Ownership.....	5
PC Checkout	5
Repair, Upgrade and Maintenance.....	5
Repurposing	5
Software	5
Substitutes	6
System Access	6
Termination/Revocation of System User Account	6
Vandalism Prohibited.....	6
Website	6

Guidelines for Acceptable Use of Tuloso-Midway Independent School District Technology Resources

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 stand-alone or networked to the District's system, without permission from the Director of Information Services.

Other issues applicable to acceptable use are:

1. Copyright: All users are expected to follow existing copyright laws.
2. Supervision and permission: Students may only use the computer network when supervised or granted permission by a staff member.
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. Internet content is filtered on the school district network. Users are prohibited from "going around" the Internet Filtering Server.
5. 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 their permission

Consequences of improper use

Improper or unethical use may result in disciplinary actions in accordance with District policies. This may include termination of employment. Additionally, individuals are subject to loss of TMISD Information Resources access privileges, and may be subject to civil and criminal prosecution. This may also require restitution for costs associated with system restoration, hardware, or software costs.

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.

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.

Electricity (clean power)

DO NOT PLUG ANYTHING OTHER THAN COMPUTERS OR PRINTERS INTO THE ORANGE OR GREY PLUGS. These electrical circuits were specially installed for computers only. They are isolated from the regular building power, and are not subject to the normal surges and sags common in normal business or residential circuits. Overheads, coffee pots, fans, refrigerators, and other appliances that are plugged into these outlets can cause surges that may affect computers elsewhere in the building.

Electronic Mail

Email has become one of the most used communications tools in both offices and classrooms. The following points are important and must be followed:

1. The following activities are prohibited by policy:
 - Sending email that is intimidating or harassing.
 - Using email for conducting personal business.
 - Using email for purposes of political lobbying or campaigning.
 - Violating copyright laws by inappropriately distributing protected works.
 - Posing as anyone other than oneself when sending email, except when authorized to send messages for another when serving in an administrative support role.
 - The use of unauthorized e-mail software.
2. The following activities are prohibited because they impede the functioning of network communications and the efficient operations of electronic mail systems:
 - Sending or forwarding chain letters.
 - Sending unsolicited messages to large groups except as required to conduct school business.
 - Sending excessively large messages.
 - Sending or forwarding email that is likely to contain computer viruses.
3. 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. Although we do not have staff who actively monitor email communications, the contents of any communication of this type would be governed by the Open Records Act. We would have to abide and cooperate with any legal request for access to email contents by the proper authorities.
4. Since email access is provided as a normal operating tool for any employee who requires it to perform their job, individual staff email addresses must be shared with interested parents and community members who request to communicate with staff in this fashion. We have no plans to produce and publish a district wide list of email addresses, but each campus and department should post a list of email addresses for their staff through their Internet pages.
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. This relates particularly to any requests for student grades, discipline, attendance or related information. In addition, security information such as username or password should not be sent via email for any reason.*
6. During student contact time in the classroom, your email notifier should be turned off to prevent interruptions. Staff members should set aside time at least once a day to check and respond to email messages. Email does not have to be answered immediately, simply allow enough time so that the 24-hour turnaround time can be met in most instances.
7. 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 picture 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.
8. Please use the “groups” function of our email system appropriately. Do not send messages to an entire staff when only a small group of people actually need to receive the message.
 9. 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.
 10. Subscriptions to Internet listservs 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.
 11. At the High School and Middle School levels, student will be issued email accounts. These accounts will be closely monitored and restricted. At the Intermediate and Primary levels, 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 technology specialist to activate a special project account for a limited time.
 12. Your username and password should be protected from unauthorized use at all times. Do not post any of this information where others can view it.
 13. Please notify your campus principal if you receive unsolicited email, particularly if it is of a “hate mail” nature. We will attempt to track down the source of that email and prevent you from receiving any additional unsolicited mail.

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 absolutely prohibited. Illegal access will result in disciplinary actions in accordance with district policies. This may include termination of employment.

Individual User Responsibilities

The following standards will apply to all users of the District's computer network systems:

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 without written permission from the campus coordinator or principal, as appropriate.
4. System users are asked to purge electronic mail or outdated files on a regular basis.
5. System users are responsible for making sure they do not violate any copyright laws.
6. System users will be responsible for the care and maintenance of their systems. Maintenance issues should be reported.

NOTE: Copies of District Policies EFE, EFE (Local), EFE (E), and EFE (E)(Local) are available at all sites.

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 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.

Information Systems Department Staff

Trish Panknin, Director of Information Services, tpanknin@tmisd.esc2.net

Orlando Pena, Network Administrator, opena@tmisd.esc2.net

Nanette Chapa, Network Technician, nchapa@tmisd.esc2.net

Ruben Rodriguez, Technician, rcervantez@tmisd.esc2.net

David Wiltshire, Technician, dwtshire@tmisd.esc2.net

Phone Number: 361-903-6415

Internet Access

All networked computers will have access to the World Wide Web. The Web is a loosely controlled collection of computers all over the world linked by special phone lines, microwave or satellite. Because there is no central control of the data available on the Internet, some information may not be considered suitable for use in schools. Although a filtering system is in place to limit access to inappropriate sites, the most important safeguard for our students is the classroom teacher. Teachers must supervise students while on the Internet, and report those students who violate the rules of the Acceptable Use Policy.

Internet Usage

- Non-business related purchases made over the internet are prohibited.
- Internet access may not be used for personal gain.
- Electronic files are subject to the same records retention rules that apply to other documents and must be retained in accordance with departmental records retention schedules.
- No files or documents may be sent or received that may cause legal liability for, or embarrassment to Tulos-Midway ISD.
- Storage of personal email messages, files and documents within TMISD's Information Resources should be nominal.
- All email messages, files and documents located on TMISD's Information Resources are owned by TMISD, may be subject to open records requests, and may be accessed in accordance with this policy.

Maintenance of Local Hard Drives

On occasion, hard drives must be reformatted. Reformatting completely erases all contents of the hard drive. All district software such as Microsoft Office, which is consistent throughout the district, will be reinstalled. All other approved software, purchased by the building, will need to be reinstalled by the campus tech specialist. Please be personally responsible for making backups of any data files that you store on your local hard drive on your campus or building server.

Network Security

Users must not install network hardware or software that provides network services with TMISD Information Services approval. Users must not download, install or run security programs or utilities that reveal weaknesses in the security of a system. For example, TMISD users must not run password cracking programs, packet sniffers, network mapping tools, or port scanners while connected in any manner to the district's network infrastructure. Users must report any weaknesses in computer security and any incidents of possible misuse or violation of this agreement to the proper authorities by contacting the Director of Information Services.

Users are not permitted to alter network hardware in any way.

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 are prohibited.
2. Pretending to be someone else when sending/receiving messages is prohibited.
3. Transmitting obscene messages or pictures is prohibited.
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.

New Equipment

All new equipment will be approved by and ordered through the Department of Information Services to ensure compatibility and inclusion in the district's central inventory.

Ownership

Electronic files created, sent, received, or stored on computers owned, leased, administered, or otherwise under the custody and control of Tulosso-Midway ISD are the property of Tulosso-Midway ISD. These files are not private and may be accessed with due cause by the Superintendent or Director of Information Services at any time without knowledge of the Information Resources user or owner. Electronic file content may be accessed by appropriate personnel in accordance with the provisions and safeguards provided in the Texas Administrative Code 201.13(b), Information Resource Standards.

PC Checkout

No computer equipment is to be taken home without filling out the proper check-out form(s) and returning to the Director of Information Services. The individual who checks it out is responsible for the safety of the equipment. Damaged or stolen items are to be repaired or replaced by the person responsible for checking it out.

Repair, Upgrade and Maintenance

All requests for service **MUST** be made by completing the online Technology Maintenance Request form. This procedure is important for tracking and verifying all work done on TMISD computers.

Repurposing

An existing computer that is replaced with a newer one will be sent to the Department of Information Services shop at the high school to be refurbished and repurposed. Computers purchased with federal funds will be repurposed for use by the federal program for which those funds were provided. On all other computers, the previous user relinquishes it upon acceptance of the new computer. A majority of these computers will be used in classrooms to meet campus requests. Do not promise your old computer to someone else.

Software

Only technology staff will be able to install or remove programs on TMISD networked computers. While this may be inconvenient to some, this is an important policy because:

- It lowers the chance that a virus will be introduced into the TMISD network.
- Users cannot accidentally install an incompatible program
- Users cannot accidentally erase all or part of an important piece of software.
- Any software that is installed by TMISD technology staff will have a legal license.
- Users must not make unauthorized copies of copyrighted software.

Software purchased for Tulosso-Midway ISD is not allowed to be installed on home computers. Programs brought from home are not allowed to be installed on TMISD computers. The district could be fined between \$10,000 and \$100,000 for each instance of an illegal software installation.

Shareware and Freeware programs, especially those downloaded from the Internet, must be judged on an individual basis by Technology staff as to safety. It is not unusual for a virus to enter a computer system through such software, and care will be taken to prevent an infection. Shareware programs, if installed, must be purchased from the author to be legally installed.

TMISD reserves the right to remove any non-business related software or files from any system. Examples of non-business related software or files include, but are not limited to: games, pop email, music files, image files, freeware and shareware.

Substitutes

TMISD teachers must have a policy for student use of computers while a substitute is in the classroom.

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 and/or supervision.
2. Teachers with accounts will be required to maintain password confidentiality by not sharing the password with students or others.
3. With the approval of the immediate supervisor, district employees will be granted access to the District's system.
4. 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.

Termination/Revocation of System User Account

The District may suspend or revoke any 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.

Vandalism Prohibited

Any malicious attempt to harm or destroy District equipment, materials or the 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 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. Vandalism as defined above will result in the cancellation of system use privileges, possible prosecution, and will require restitution for costs associated with system restoration, hardware, or software costs.

Website

The district's website is: www.tmisd.esc2.net