Acceptable Use Policy

Acceptable Use Policy For Matagorda Independent School District Employees

Access to Matagorda ISD's network, devices and technology resources is a privilege, not a right. **All users shall be required to acknowledge receipt and understanding of all administrative regulations governing use of the District's technology resources and shall agree in writing to allow monitoring of their use and to comply with such regulations and guidelines. Noncompliance may result in suspension of access or termination of privileges and other disciplinary action consistent with District policies**. [See DH, FN series, FO series, and the Student Code of Conduct] Violations of law may result in criminal prosecution as well as disciplinary action by the District.

At MISD, we will use network, devices and technology resources as one way of enhancing the mission to teach the skills, knowledge and behaviors students will need to succeed in the global community. These technologies include all district-provided equipment such as computers, tablets, cell phones, laptops, netbooks, e-readers, iPads, and more.

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 regarding the use of the District's system will emphasize the ethical use of this resource.
In accepting this agreement, students, faculty and staff acknowledge the following:

Internet Safety Procedures

It is the policy of Matagorda ISD to:

(a) prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications; (b) prevent unauthorized access and other unlawful online activity; (c) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and (d) comply with the Children's Internet Protection Act [Pub. L. No. 106-554 and 47 USC 254(h)].

Access to Inappropriate Material

To the extent practical, technology protection measures (or "Internet filters") shall be used to block or filter Internet, or other forms of electronic communications, access to inappropriate information. Specifically, as required by the Children's Internet Protection Act, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors. Subject to staff supervision, technology protection measures may be disabled for adults or, in the case of minors, minimized only for bona fide research or other lawful purposes.

Inappropriate Network Usage

To the extent practical, steps shall be taken to promote the safety and security of users of the MISD online computer network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications. Specifically, as required by the Children's Internet Protection Act, prevention of inappropriate network usage includes: (a) unauthorized access, including so-called 'hacking,' and other unlawful activities; and (b) unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

Education, Supervision and Monitoring

It shall be the responsibility of all members of the MISD staff to educate, supervise and monitor appropriate usage of the online computer network and access to the Internet in accordance with this policy, the Children's Internet Protection Act, the Neighborhood Children's Internet Protection Act, and the Protecting Children in the 21st Century Act. Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of campus principals or designated representatives.

The campus principals or designated representatives will provide age appropriate training for students who use the MISD Internet facilities. The training provided will be designed to promote the MISD commitment to:

a. The standards and acceptable use of Internet services as set forth in the
MISD Internet Safety Procedures;

b. **Student safety with regard to:**

- **safety on the Internet;**
- **appropriate behavior while on online, on social networking Web sites, and**
- **in chat rooms; and**
- **cyberbullying awareness and response**.

c. Compliance with the E-rate requirements of the Children's Internet Protection Act
("CIPA"). Following receipt of this training, the student will acknowledge that he/she received the training, understood it, and will follow the provisions of the District's acceptable use policies.

Copyright

All persons are prohibited from using District technology in violation of any law including copyright laws. Only appropriately licensed programs or software may be used with District technology resources. No person shall use the District's technology resources to post, publicize, or duplicate information in violation of copyright law. The Board shall direct the Superintendent or designee to employ all reasonable measures to prevent the use of District technology resources in violation of the law. All persons using District technology resources in violation of law shall lose user privileges in addition to other sanctions.
Unless a license or permission is obtained, electronic media in the classroom, including motion pictures and other audiovisual works, must be used in the course of face-to-face teaching activities as defined by law.

Electronic Mail

All network users are provided with an email account for use in conjunction with their job. An assigned email account is the property of MISD.

1. **While email can be a valuable tool, the following activities are prohibited by policy:**

- Sending email that is intimidating or harassing, abusive, threatening, obscene, sexually oriented, discriminatory, damaging, illegal, false, profane, or any other inappropriate behavior.
- Using email for conducting personal business or 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.
- Using another employees email account.
- 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.

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, virus warnings, urban legends or other unsubstantiated scares.
    - 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 the campus should post a list of email addresses for their staff through their Campus webpages.

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.

Electronic Media

An employee wishing to express concern, complaints, or criticism shall do so through appropriate channels and not any form of electronic media which includes all forms of social media, such as text messaging, instant messaging, electronic mail (e-mail), Web logs (blogs), electronic forums (chat rooms), video-sharing Web sites, editorial comments posted on the Internet, and social network sites. Electronic media also includes all forms of telecommunication, such as landlines, cell phones, and Web-based applications. An employee shall be held to the same professional standards in his or her public use of electronic media as for any other public conduct. If an employee's use of electronic media violates state or federal law or District policy, or interferes with the employee's ability to effectively perform his or her job duties, the employee is subject to disciplinary action, up to and including termination of employment.

Use with Students:

- The employee shall limit communications to matters within the scope of the employee's duties. For an employee with an extracurricular duty, communication should be limited to matters, relating to the extracurricular activity.
- **The employee does not have a right to privacy with respect to communications with students and parents.**
- The employee continues to be subject to applicable state and federal laws, local policies, administrative regulations, and the Code of Ethics and Standards practices for Texas Educators:
    - Compliance with the Public Information Act and the Family Educational Rights and Privacy Act (FERPA), including retention and confidentiality of student records
    - Copyright Law
    - Compliance with the Children's Internet Protection Act (CIPA)

Employees are personally responsible for the content they publish online. Be mindful that what you publish will be public for a long time, protect your privacy.

- Your online behavior should reflect the same standards of honesty, respect, and consideration that you use face-to-face.
- Remember that these sites are an extension of your profession. What is inappropriate in your workplace should be deemed inappropriate online.
- The lines between public and private, personal and professional are blurred in the digital world. By virtue of identifying yourself as TMISD employee online, you are now connected to colleagues, students, parents and the school community. You should ensure that content associated with you is consistent with your work at Matagorda ISD.
- Employees shall not use the MISD district's logo or other copyright materials of the MISD district without express, written consent.
- **When contributing online, do not post confidential student information.**
- **Employees must not use social-networking sites to disparage the schools, its students, programs, activities, volunteers, or other employees.**
- **Accessing and posting to social networking sites during the work day from any device is prohibited.**
- **Employees must not communicate with students from their personal social-networking sites.**

Any employee found to be in violation will be subject to immediate disciplinary action, up to and including termination of employment. In addition, the school reserves the right to publicly access an employee's electronic media sites as part of its decision-making process with respect to promotions and other human relations managements requirements and considerations. Where applicable, employees may be asked to provide access as part of an employment selection and/or promotion process.

Internet Access/Filtering

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. A filtering system within our district and at our Educational Service Center implements measures to protect K-12 school children from harmful online content/inappropriate matter as required by the Children's Internet Protection Act (CIPA). These filters protect against access by adults and minors to visual depictions that are obscene, pornographic, inappropriate for students, or harmful to minors. 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. The district will disable the filter upon request for all staff with a justified request for "bona fide research or other lawful purposes". This request must be made in writing to the head campus administrator. All request must contain the link, include the justification and duration of the time to unblock.

Internet Usage

- Non-business related purchases made over the internet are prohibited.
- Internet access may not be used for personal gain.
- Any device that is not the property of MISD is prohibited and not allowed on the district network
- 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 Matagorda ISD.
- Storage of personal email messages, files and documents within MISD's Information Resources should be nominal.
- All email messages, files and documents located on MISD's Information Resources are owned by MISD, may be subject to open records requests, and may be accessed in accordance with this policy.
- Any mobile internet access (i.e. 3G-4G) activation will be the responsibility of the user and not the school district. All district owned devices warrant that users understand and agree to comply with all rules and regulations of the Acceptable Use Policy at home or the work place.

Maintenance of Local Hard Drives

On occasion, hard drives must be reformatted or replaced. 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 campus, will need to be reinstalled by the Network Technician. You will be personally responsible for making backups of any personal data files that you store on your local hard drive on your campus or building server.

Network Security

Student/Teacher personal owned devices are prohibited and should NEVER be connected to the schools wired network or wireless networks in the district. Other prohibited equipment is any network attached items including, but not limited to: hubs, switches, routers, wireless access points, splitters, network printers, key loggers, personal PCs, laptops, or iPads. Additions of any type of these items are prohibited. Persons who introduce these devices on the Network will be subject to denial of access, and disciplinary actions, including termination for employees.

Users must not install network hardware or software that provides network services without the MISD Technology Department approval. Users must not download, install or run security programs or utilities that reveal weaknesses in the security of a system. For example, MISD 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 Technology Coordinator.

Monitored Use

Electronic files created, sent, received, or stored on computers owned, leased, administered, or otherwise under the custody and control of Matagorda ISD are the property of Matagorda ISD. These files are not private and may be accessed and monitored by the Superintendent or Technology Department at any time without knowledge of the user or owner to ensure appropriate use. 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.

Stolen or Damaged Technology

Damaged or stolen items are the responsibility of the user to report to the principal and technology department immediately. If there is a police report filed, a copy of the report must be made available to the Technology Coordinator. Various technologies can be tracked and the police report will be helpful in tracking these devices. Any school-owned technology equipment in the hands of a school-owned employee becomes the liability of the school employee. The employee accepts all responsibility for replacement costs due to theft, loss or damage. The employee will be liable for payment of all replacements or repairs. Repair costs will be deducted from the employee's check or the employee can pay all of the costs at one time. Failure to report stolen, lost or damaged equipment will result in the cost of the equipment being deducted from the employee's paycheck.

Maintenance Requests/Inventory

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 MISD computers. If an online Technology Maintenance Requests form is not completed, the Technology Department may not honor your request for service. All technology will be tracked and must be verified to keep accurate inventory. Under no circumstances should any technology be moved within the district or campus without the permission of the technology department. All technology will remain in the classroom as stated in the inventory. Proper forms, available through the Campus Technology Specialists must be filled out and approved by the principal before the Campus Techs can move technology to another room or campus.

Software

Only technology staff will be able to install or remove programs on MISD 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 MISD 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 MISD technology staff will have a legal license.
- Users must not make unauthorized copies of copyrighted software.
- **Download of movies or music without administrative permission**

Software purchased for Matagorda ISD is not allowed to be installed on home computers. Programs brought from home are not allowed to be installed on MISD 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 the safety. It is not unusual for a virus to enter a computer system through such software, and precautions will be taken to prevent an infection. Shareware programs, if installed, must be purchased from the author to be legally installed.

MISD 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.

An employee or student knowingly bringing prohibited materials into the school's electronic environment will be subject to disciplinary action in accordance with policy.

Substitutes

MISD teachers must have a lesson plan for student use of computers while a substitute is in the classroom. Short term substitutes or student teachers will not be given access to our network.

Network Access

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

- Students will have access to the District's resources for class assignments and research with their teacher's permission and/or supervision.
- Teachers with accounts will be required to maintain password confidentiality by not sharing passwords with students or others.
- Computers should be locked or logged off when you are not at your desk.
- If a password is forgotten or has been compromised, please contact the technology department.
- Any network user identified as a security risk or having violated District Acceptable Use Guidelines may be denied access to the District's network system. Other consequences may also be assigned.

Termination/Revocation of Network User Account

The District may suspend or revoke any network user's access to the District's network 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 network privileges, or on a future date if so specified in the notice. An employee who is terminated must return all equipment in the employee's possession. If an employee fails to return any equipment, the monetary value of the equipment will be deducted from the employee's final paycheck.

Vandalism Prohibited

Any malicious attempt to harm or destroy District equipment, materials, data of another user system, or any of the agencies or other networks to which the District has access is prohibited. Deliberate attempts to degrade or disrupt network 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 network use privileges, possible prosecution, and will require restitution for costs associated with network restoration, hardware, and/or software costs.

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 MISD 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, and/or software costs.

Disclaimer of Liability

The District shall not be liable for users' inappropriate use of the District's technology resources, violations of copyright restrictions or other laws, users' mistakes or negligence, and costs incurred by users. The District shall not be responsible for ensuring the availability of the District's technology resources or the accuracy, age appropriateness, or usability of any information found on the Internet.
Record Retention
All electronic records shall be retained, whether created or maintained using the District's technology resources or using personal technology resources, in accordance with the District's record management guidelines.

Website

The district's website is:matagordaisd.org

Acceptable Use Agreement

I have read and agree to follow the attached Acceptable Use policy. I also understand that if I fail to follow these policies I may lose access to District technology and may be reprimanded. If I lose or destroy District technology, I am responsible to reimburse the District for the cost of that technology.

____

Student / Employee   Date

____

Parent of Student   Date