

MCGREGOR I.S.D.
Electronic Communication and Data Management Policy

Regulations for Acceptable Use

PHILOSOPHY AND PURPOSE

The District provides technology resources to its students and staff for educational and administrative purposes. The goals in providing these resources are:

1. Promote educational excellence in its schools by facilitating resource sharing, innovation, and communication.
2. Improve learning and reach the District's instructional goals.
3. Achieve effective and efficient administration at the District and campus levels.
4. Comply with the Texas Education Agency's guidelines for technology in schools.

Any use of the district's electronic information systems and resources by authorized users must be in furtherance of these limited purposes and conform to the District's expectations for legal, efficient, and ethical use.

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.

INTERNET SAFETY AND LIMITATIONS ON SITE ACCESS

Recognizing that the Internet can give access to sites containing information that is obscene, child pornography, or harmful to minors or that would be otherwise inappropriate for distribution to students, unsuitable for use in the approved curriculum, or irrelevant to accomplishing the district's stated purposes for operating an Internet-accessible network, the District has installed technology protection measures, as defined by the federal Children's Internet Protection Act, to filter, screen, analyze, and block site content in an effort to make it more difficult for students or staff to gain access to such material through the District's network.

The Technology Director or designated campus administrators may disable technology protection measures during use by an adult to allow access to otherwise prohibited or blocked sites or information for bona fide research or other acceptable purposes under this policy.

Nonetheless, the District makes no representation that it can control access to all Internet sites. Network users are responsible for their actions in accessing available resources and will be held accountable for receiving information that is inconsistent with the requirements for acceptable and unacceptable use of the network and Internet.

AUTHORIZED USERS

The District permits its students and staff to become authorized users of the computer network and/or have access to the Internet, subject to administrative regulations developed by the Technology Director and approved by the Superintendent.

To become an authorized user, a person must sign the appropriate User Agreement and return the form to the Technology Director or designee. Minor students applying for a user account must return a User Agreement signed by their parent/guardian and themselves.

Staff and students are responsible for the care and maintenance of their network, computer, and email accounts. Each authorized user is responsible for all activities, transmissions, or actions that occur during the use of their accounts. Password confidentiality of all assigned accounts must be maintained. Personal account sharing is prohibited. Account maintenance consists of deleting unnecessary files on a regular basis.

GENERAL REQUIREMENTS FOR NETWORK AND INTERNET USE

Student and employee use of the District's computer network and/or access to the Internet must be in accordance with this policy and must be conducted on a district computer workstation. Due to security issues, the use of personal computers and other telecommunication devices (i.e., laptops, handheld computers, cell phones, gaming devices, personal digital devices, etc.) on the District's network is prohibited. Should a situation prompt the use of a personal device previously mentioned, the user must make a formal request to the District Technology Department for authorization of temporary use.

Access to the District's electronic communications system, including the Internet, shall be made available to members of the public, as deemed necessary and in accordance with administrative regulations. Such use may be permitted as long as 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 administrative approval.

Any user who identifies a security problem with the network must immediately notify the District Technology Director and may not communicate the problem to any other person.

MONITORING USE

Use of a personal network account through the District's system is voluntary and constitutes a privilege provided by the District, not a right. All network usage is subject to monitoring, examination, and investigation by the system administrators without prior notice or the specific consent of the user. By signing the User Agreement, each authorized user acknowledges the possibility of such monitoring and consents to it.

Professional employees overseeing student use of the District's computer network or access to the Internet will be vigilant in determining that students are using the District's system only in compliance with this policy to enhance student safety and security, particularly when students are using the Internet, electronic mail, chat rooms authorized under this policy, and other forms of direct electronic communication.

SUSPENDING OR REVOKING PRIVILEGES

Access to the network, the Internet, or both may be suspended or revoked and user accounts deleted if a student or employee is determined to have violated this policy or the User Agreement each user signs as a condition for obtaining access to the District's network and/or the Internet.

Any user identified as a security risk or who has a history of violations with other computer systems will be denied access to the network. A user whose access has been suspended or revoked may request a conference with the principal and Technology Director to discuss the basis for that action and have an opportunity to respond. A decision by the Technology Director to suspend or revoke system privileges may be appealed to the Superintendent or the Board. System privileges are revoked during any appeal.

ACCEPTABLE USE

Any use described below is deemed "acceptable" and consistent with the User Agreement and this policy. The final decision regarding whether any given use of the network or Internet is acceptable lies with the Superintendent or designee, in consultation with the District Technology Director.

1. Supports instructional purposes and goals.
2. Furthers the District's educational and administrative purposes, goals, and objectives.
3. Furthers research related to education and instruction.
4. Does not violate the student code of conduct or employee standards of conduct.
5. Is consistent with network rules established by the District Technology Director.

Podcasts are allowed as long as the podcast is student or teacher created and is in support of district goals and/or supports approved curriculum.

Blogs, forums, and Wikis are allowed as long as the postings are student or teacher created and are in support of district goals and/or supports approved curriculum. Users must use the Blog and/or Wiki service provided by the District unless otherwise approved by the Technology Director.

Creation of teacher/staff web sites utilizing the District's web service is encouraged. Users must attend a formal web site training session and sign the Web Site Guidelines Agreement. Resources and materials posted online must be published on the District web server and in accordance with approved web publishing guidelines.

UNACCEPTABLE USE

Any of the following uses is deemed "unacceptable" and a violation of the User Agreement and this policy. The final decision regarding whether any given use of the network or Internet is unacceptable lies with the Superintendent or designee, in consultation with the District Technology Director.

1. Unauthorized use of copyrighted material, including violating District software licensing agreements.
2. Unauthorized download or installation of any software for use on MISD computers. This pertains to freeware, shareware, and all other forms of software and files not directly related to the instructional and administrative purposes of the District.
3. Posting or distribution of threatening, racist, harassing, excessively violent, or obscene material.
4. Personal, political use to advocate for or against a candidate, office-holder, political party, or political position. Research or electronic communications regarding political issues or candidates shall not be a violation when the activity is to fulfill an assignment for class credit.
5. Participating in social networking, instant messaging, or chat enabled sites other than those authorized by the District Technology Department.
6. Tampering, i.e., accessing, reading, deleting, copying, or modifying, with the electronic mail of other users, regardless of where the message is displayed or stored.
7. "Hacking," i.e., attempting unauthorized access to any computer whether within the District's network or outside it.
8. Use of the network to access or process pornographic material, inappropriate text files, or files dangerous to the integrity of the local area network.
9. Establishing network or Internet connections to live communications, including voice and/or video other than those communications authorized by the District Technology Department.
10. Efforts to bypass or disable network and/or Internet filtering or security measures.
11. Games are prohibited unless specifically authorized by a teacher for instructional purposes.
12. Any use that would be unlawful under state or federal law.
13. Unauthorized disclosure, use, or distribution of personal identification information regarding students or employees.
14. Forgery of electronic mail messages or transmission of unsolicited junk e-mail chain messages.
15. Use that violates the student code of conduct or employee standards of conduct.
16. Use related to commercial activities or for commercial gain by a student or employee.
17. Excessive personal use of the District's network, Internet, and email systems.

SERIOUS VIOLATIONS

If the principal determines that a student's or employee's use of the system violates the student code of conduct or employee standards of conduct and that disciplinary action other than or in addition to suspension or revocation of system privileges is warranted, those disciplinary actions will be in accordance with the applicable policies.

SYSTEM OR OTHER USER INTERFERENCE

Users must not attempt to exceed, evade, or change established resource quotas, i.e., allocations of local hard drive storage space or network time. The District quotas are designed to ensure all users have a fair opportunity to access resources.

Vandalism and mischief are prohibited. Vandalism includes any attempt to harm or destroy another user's data on the network or on any network connected to the District's network and any deliberate creation or propagation of a computer virus(es). Mischief includes any interference with another user's work, such as attempts to delete, examine, copy, or modify data, files, fields, or any other element of another user's information. Vandalism and mischief as defined above will result in cancellation of system use privileges. The party will be responsible for restitution costs associated with system restoration, hardware, or software costs.

DISCLAIMER

The District makes no warranties of any kind, expressed or implied, for its network facilities and bears no liability for users' copyright violations; user's inappropriate or tortious use of the network system or resources; any damages incurred by users, including loss of data resulting from the action or inaction of any District employee or

a user's errors or omissions; and phone charges, credit card charges, or any other charges incurred by users without prior District authorization and according to established purchasing procedures. The District specifically denies any responsibility for the accuracy, age-appropriateness, or quality of information obtained through its network facilities.

INTELLECTUAL PROPERTY RIGHTS

Students retain the copyright and all other intellectual property rights to works of any kind they create using the District's electronic information resources and system, including those created in fulfillment of course requirements or through participation in extracurricular activities. The District is the copyright owner of any work created or developed by an employee within the scope of his or her employment, regardless of whether the work is prepared at school using school equipment or out of school using personally owned or other equipment.

Employee User Agreement
District Network and Internet Resources

I have read the Network and Internet Use policy [CQ (LOCAL)] attached to this agreement and understand the conditions for use of the network and Internet resources provided by McGregor I.S.D. for the purpose of promoting educational excellence and supporting instructional goals.

By my signature below, I agree that any use of the network and Internet under my personal network, computer, and email accounts will be consistent with that policy. **I understand that the District Technology Department has the authority to and will monitor network usage, including electronic messages sent and received to ensure compliance with the policy, and by this Agreement consent to that access.** Furthermore, I understand that I am responsible for any transactions that occur under my personal accounts mentioned above and that any violation of that policy shall be considered misconduct and a violation of the employee standards of conduct.

Employee's Signature

Date

Employee's Name, Printed

Campus

Parent Information and Authorization

District Network and Internet Resources

McGregor I.S.D. provides an array of technology resources for student use as part of its overall instructional program and for the purposes specified in the attached Network and Internet Use policy [CQ (LOCAL)]. It is important that the student and parent/guardian read the policy to know and understand the appropriate use and prohibited activities when using these technology resources.

=====

I have read the Network and Internet Use policy [CQ (LOCAL)] within the Student Handbook and understand the conditions for use of the network and Internet resources provided by McGregor I.S.D. for the purpose of promoting educational excellence and supporting instructional goals.

By my signature below, I consent to my child, having access to the Internet through the McGregor I.S.D. network and release the school district from any responsibility for information my child may obtain in the course of using the Internet.

Further, I agree that any use of the network and Internet under my child's class account and/or personal network, computer, and email account must be consistent with that policy. I understand that district employees have the authority to and will monitor network usage, including electronic messages sent and received to ensure compliance with the policy, and by this Agreement consent to that access.

I understand that my child is responsible for any transactions that occur during the use of his/her personal network, computer, and email accounts, as well as his/her use of the network and/or Internet. I understand that any violation of that policy will be considered a violation of the Student Code of Conduct, and that my child may be denied access to the district's network system as well as electronic resources in addition to any other disciplinary action.

Parent's Signature

Date

Parent's Name, Printed

Student's Signature

Date

Student's Name, Printed

Grade Level

Campus

Homeroom Teacher (Elem. only)

McGregor ISD does not discriminate on the basis of sex, disability, race, color, age, or national origin in its educational programs, activities, or employment as required by Title IX, Section 504, and Title VI.