Mathis Independent School District
602 East San Patricio, Mathis TX, 78368
Phone: 361.547.3378
Fax: 361.547.9474

Acceptable Use Policy

1.0 Overview
The Technology Department's intention for publishing an Acceptable Use Policy is not to impose restrictions that are contrary to Mathis I.S.D.'s established culture of openness, trust and integrity. The Technology Dept. is committed to protecting Mathis I.S.D.'s employees, students and the District from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of Mathis I.S.D. These systems are to be used for business and educational purposes in serving the interests of Mathis I.S.D. in the course of normal operations.

Effective security is a team effort involving the participation and support of every Mathis I.S.D. employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2.0 Purpose
The purpose of this policy is to outline the acceptable use of computer equipment at Mathis I.S.D. These rules are in place to protect the employee and Mathis I.S.D. Inappropriate use exposes Mathis I.S.D. to risks including virus attacks, compromise of network systems and services, and legal issues.

3.0 Scope
This policy applies to employees, contractors, consultants, temporary, and other workers at Mathis I.S.D., including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Mathis I.S.D.

4.0 Policy
4.1 General Use and Ownership

1. While Mathis I.S.D.'s network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the District systems remains the property of Mathis I.S.D. Because of the need to protect Mathis I.S.D.'s network, management cannot guarantee the confidentiality of information stored on any network device belonging to Mathis I.S.D.
2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use.
3. The Technology Dept. recommends that any information that users consider sensitive or vulnerable be encrypted.
4. For security and network maintenance purposes, authorized individuals within Mathis I.S.D. may monitor equipment, systems and network traffic at any time, per Technology's Audit Policy.
5. Mathis I.S.D. reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

1. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. Malicious users may gain access to your information if you chose to give your credentials to an individual. Please see the District Password Policy for more information or clarification.
2. All PCs, laptops and workstations should be secured with a password-protected device with the automatic activation feature set at 15 minutes or less, or by logging-off when the host will be unattended. Malicious users can send messages in your name or access potentially confidential

information if you leave yourself logged in to your computer and walk away. The logged in user is responsible for any malice that may be done on their computer while left unattended.
3. Because information contained on portable computers is especially vulnerable, special care should be exercised.
4. Postings by employees from a Mathis I.S.D. email address should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Mathis I.S.D., unless posting is in the course of business duties.
5. All hosts used by the employee that are connected to the Mathis I.S.D. Internet/Intranet/Extranet, whether owned by the employee or Mathis I.S.D., shall be continually executing approved virus-scanning software with a current virus database.
6. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, Trojan horse code, or Phishing forms.
7. For security reasons, Administrator Rights are given to the Technology Department (for installation and administration of the computer system) and individuals designated by the Superintendent. For more information, please see the following link on why you DO NOT want administrator rights to your computer. http://blog.paradigmcc.com/2009/05/14/why-you-do-not-want-administrative-rights-on-your-computer/

4.3. Unacceptable Use
The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of Mathis I.S.D. authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Mathis I.S.D.-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities
The following activities are strictly prohibited:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Mathis I.S.D.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Mathis I.S.D. or the end user does not have an active license is strictly prohibited.
3. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.)
4. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
5. Using a Mathis I.S.D. computing asset to actively engage in producing, viewing, downloading, uploading, or streaming, or transmitting material that is of a pornographic or sexual nature that is not tied to the District curriculum.
6. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not

limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
7. Port scanning or security scanning is expressly prohibited.
8. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
9. Circumventing user authentication or security of any host, network or account. This includes the use of any proxy software or website.
10. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
5. Use of unsolicited email originating from within Mathis I.S.D.'s networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Mathis I.S.D. or connected via Mathis I.S.D.'s network.
6. Sending sensitive staff or student information over email. Depending on the content of the email, an email may be considered an educational record, and as such must be treated as any other educational record under FERPA. Keep in mind that email:
   - Can be unsecured on a computer
   - Can be accessed from remote locations
   - Can be subpoenaed
   - Can be requested under the Texas Open Records Act
   - Is transmitted in clear text while it travels over the internet (i.e. it is like sending a post card, any one on the internet can see and read it while it is in transit.)

   Staff can be held personally, financially, and legally responsible under FERPA (Federal Education Rights and Privacy Act) for divulging protected individuals' personal information.

   Professional certificates can be revoked by TEA due to FERPA violations.

4.4. Blogging

1. Blogging by employees, using Mathis I.S.D.'s property and systems is subject to the terms and restrictions set forth in this Policy. Use of Mathis I.S.D.'s systems to engage in blogging is acceptable, and encouraged, provided that it is done in a professional and responsible manner, does not otherwise violate Mathis I.S.D.'s policy, is not detrimental to Mathis I.S.D.'s best interests, and does not interfere with an employee's regular work duties. Blogging from Mathis I.S.D.'s systems is also subject to monitoring.
2. Blogging by employees, using systems other than those own or operated by Mathis I.S.D., are also subject to the terms and restrictions set forth in both this Policy and the section of the Employee Handbook entitled "Personal Use of Electronic Media."
3. Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of Mathis I.S.D. and/or any of its employees or students. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by Mathis I.S.D.'s Discrimination, Harassment, and Retaliation Policy.

Mathis Independent School District
602 East San Patricio, Mathis TX, 78368
Phone: 361.547.3378
Fax: 361.547.9474

4. Employees may also not attribute personal statements, opinions or beliefs to Mathis I.S.D. when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of Mathis I.S.D. Employees assume any and all risk associated with blogging.

5.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6.0 Definitions

Term	**Definition**
Blogging	Writing a blog. A blog (short for weblog) is a personal online journal that is frequently updated and intended for general public consumption.
Spam	Unauthorized and/or unsolicited electronic mass mailings.

_____ _____
Employee Signature Date

_____
Employee Name

Revision History
February 1, 2011 Initial Revision