

TECHNOLOGY PRIVACY AND ACCEPTABLE USE POLICY

1.0 Overview

The Madison-Plains Local School District (herein “the District”) provides technology access to students to advance educational opportunities. The District will do everything within its control to provide students with a safe, healthy learning environment. All devices, District-Owned and Personal, must follow the guidelines of this policy and the student handbook. The District reserves the right to inspect, copy, and/or delete records referenced through technological property. Technology use is a privilege and is not guaranteed for those who violate District Policies. Students are permitted to use personal technology devices at the discretion of school personnel.

2.0 General Guidelines

1. Be polite. Use appropriate language. No swearing, vulgarities, suggestive, obscene, or threatening language.
2. Do not share personal account information or allow others to use your account.
3. Do not reveal personal information unless it is for educational purposes with trusted individuals/agencies.
4. Using technology resources to participate in Cyber-Bullying is not permitted. “Cyber Bully” means any threats, harassment, or intimidation of another person through the use of technology.
5. Do not violate any copyright or similar laws or regulations, including, but not limited to those of magazines, books, music, the installation or distribution of "pirated" software, or software not appropriately licensed.
6. Do not buy or sell anything through the use of technology while using or on District property.
7. Do not assume someone that sends an e-mail is giving his or her permission for you to forward or redistribute the message.
8. Access of non-educational social networking web sites during school hours is prohibited.
9. Staff shall report any actions by others that would violate the security or integrity of any technology device, networking, or messaging system to a teacher or principal immediately.
10. Students are prohibited from posting information, photographs, or inappropriate information on any website that might result in a disruption of the educational environment or District activity.
11. The district is not responsible or liable for student’s personal electronic devices.

3.0 Internet / Network Security

The District uses internet filtering/security to protect its network and prevent students, employees or other users from viewing undesirable content. This filtering software is required by law (Child Internet Protection Act) as a means to protect the District’s students. At no time is any District staff/student/visitor permitted to circumvent this software to access a denied site or service. Policies include, but are not limited to:

1. Distributing or utilizing internet “proxy” sites to circumvent District network filtering or security.
2. Installing or using unauthorized software on District-Owned equipment.
3. Using, accessing, or distributing profane or obscene material, material suggesting illegal acts and/or material advocating violence or discrimination. Special permission can be granted by the Building Principal upon special request for educational purposes.
4. Intentionally wasting limited resources such as network bandwidth, disk space, and/or consumables (e.g., Non-Educational Games, Printer Ink, etc.)
5. Utilizing any device/resource to cause technology outages or interruptions.

6. Introduction of malicious programs or devices onto the District's Network that could cause a disruption. These include, but are not limited to, viruses, worms, trojan horses, spyware, or unauthorized network devices (Access Point/Internet Connection Sharing/Router).
7. Executing any form of network monitoring in aims of spying/intercepting data not intended for the student's technology device.
8. Posting false or defamatory information
9. Plagiarizing information found on the internet.
10. Damaging, tampering with, or reallocating District technology property.

4.0 Email / Messaging

Student access to e-mail is a privilege with a degree of responsibility for the user. As an instructional tool, student email accounts are monitored and controlled by the District.

Policies include, but are not limited to:

1. Email must be appropriate and non-offensive.
2. Messages must not contain profanity, obscene comments or sexually explicit materials.
3. Messages must not contain racist, sexist, religious or generation derogatory content. Respect for members of the school and general community is expected and should be expressed.
4. User identity will be accurately reflected in all message traffic.
5. No virus, program, or addition will be introduced into the system which alters its operations, destroys, or damages data, or renames or relocates files.
6. No unsolicited e-mail messages, including the sending of "junk mail", chain letters, or other advertising material to individual who did not specifically request such material (e-mail/spam).
7. Be considerate when sending attachments with e-mail (where this is permitted). Be sure that the file is not too large to be accommodated by the recipient's system and is in a format which the recipient can open.
8. Any form of harassment or cyber-bullying via e-mail, telephone or messaging, whether through language, frequency, or size of messages is prohibited.

5.0 Right of Access

Although the Board respects the natural desire of all persons for privacy in their personal communications, and will attempt to preserve this privacy whenever possible, the operational and security needs of the District's computer network and messaging systems require that full access be available at all times. The District therefore reserves the right to access and inspect any computer, device or electronic media within its systems and any data information, or messages which may be contained therein. All such data, information, and messages are the property of the District. Students should have no expectation that any information on the District's network or devices will remain private.

6.0 Consequences for Technology Violations

Penalty for infractions will be applied based upon the degree of the offense by: Teacher, Principal or Technology Coordinator

PARENT RELEASE FOR INTERNET/E-MAIL:

By signing a release form, because access to on-line services provides connections to other computer systems located all over the world, users (and parents of users, if the user is under 18 years old) must understand that neither the school nor the district can control the content of the information available on these systems. Some of the information available is controversial and offensive. The district does not condone the use of such materials. School employees, students and parents of students must be aware that the privileges to access computers and/or on-line

services will be withdrawn from users who do not respect the rights of others or who do not follow the rules and regulations established by the Board of Education.

Parents wishing to limit their child's use of the Internet of Messaging must send a signed letter to the Principal requesting that permission be limited by resource.

PARENT RELEASE FOR MEDIA DISTRIBUTION:

By signing a release form, the parent/guardian grants permission to the District to use the image of their child. Such unrestricted use includes the display, distribution, publication, transmission or otherwise use of photograph, images and/or video taken of students for use in materials such as newsletters and brochures, videos, and digital images such as those on Madison-Plains Local Schools website. There will be no financial compensation for recorded images.

Parents wishing to deny permission must send a signed letter to the Principal requesting that permission be denied to use their child's image on the District's website or new releases.