Technology Use Policy

Written by GMRSD Webmaster

INTRODUCTION:

The Gill-Montague Regional School District shall provide access for employees and students to the system/network, including access to external networks, for limited educational purposes.

Educational purposes shall be defined as classroom activities, career and professional development, and high quality self discovery activities of an educational nature. The purpose of the system/network is to assist in preparing students for success in life and work by providing access to a wide range of information and the ability to communicate with others. The system/network will be used to increase communication (staff, parent, and student), enhance productivity, and assist staff in upgrading existing skills and acquiring new skills through a broader exchange of information. The system/network will also be utilized to provide information to the community, including parents, governmental agencies, and businesses.

Availability

The Superintendent or designee shall implement, monitor, and evaluate the district's system/network for instructional and administrative purposes.

Access to the system/network, including external networks, shall be made available to employees and students for instructional and administrative purposes and in accordance with administrative regulations and procedures.

Access to the system/network is a privilege, not a right. All users shall be required to acknowledge receipt and understanding of all administrative regulations and procedures governing use of the system and shall agree in writing to comply with such regulations and procedures. Noncompliance with applicable regulations and procedures may result in suspension or termination of user privileges and other disciplinary actions consistent with the policies of the Gill-Montague Regional School District. Violations of law may result in criminal prosecution as well as disciplinary action by the Gill-Montague Regional School District.

Acceptable Use

The Superintendent or designee shall develop and implement administrative regulations, procedures, and user agreements, consistent with the purposes and mission of the Gill-Montague Regional School District as well as with law and policy governing copyright.

Monitored Use

Electronic mail transmissions and other use of electronic resources by students and employees shall not be considered confidential and may be monitored at any time by designated staff to ensure appropriate use for instructional and administrative purposes.

Liability

The Gill-Montague Regional School District shall not be liable for users' inappropriate use of electronic resources or violations of copyright restrictions, users' mistakes or negligence, or costs incurred by users. The Gill-Montague Regional School District shall not be responsible for ensuring the accuracy or usability of any information found on external networks.

ACCEPTABLE USE POLICY - TECHNOLOGY

(from GMRSD Policy Manual, section IJNDB-R)

I. Introduction

The Gill-Montague Regional School District provides electronic resources to:

- Improve education for all students through access to unique resources and partnerships.
- Improve learning and teaching through research, teacher training, collaboration and distribution of successful education practices, methods, and data.

Our electronic resources include, but are not limited to:

- Wired and wireless network infrastructure
- Internet connectivity
- Computer workstations
- Laptop computers
- Terminal and “thin client” stations
- Any tablet or mobile device including mobile phones.
- Network data storage
- Network application services
- Email
- Cloud hosted services
- District and school web pages.

We seek to ensure a healthy and appropriate use of these resources by making provisions for:

- Prevention of access by minors to inappropriate matter on the Internet
- The safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications.
- Prevention of unauthorized access and use of technology resources.
- Prevention of unauthorized disclosure, use and dissemination of personal information regarding minors.

II. General provisions

A. Network monitoring

Any activity while using district electronic resources is subject to monitoring and reporting at the discretion of District Administration. Users should have no expectation of privacy when browsing the web, sending or receiving e-mail, or using any other electronic resources provided by the District.

B. Internet Content Filtering

In accordance with the Children's Internet Protection Act (CIPA), passed by the U.S. Legislature in January 2001 (Public Law 106-554), our schools shall employ filtering software to block access to inappropriate content on all computers with Internet access. Our schools and districts certify that a policy of Internet safety and technology protection measures shall be enforced. Users are restricted from accessing visual depictions of subject matter that is obscene, pornographic, child pornographic or harmful to minors. In compliance with CIPA our schools and districts shall, in furtherance of this policy of Internet safety, monitor the online activities of minors.

The District and its schools cannot be held responsible for misuse of material downloaded from any online service, or for inappropriate or sexually explicit material being obtained through any district electronic resource.

C. Students, staff, and parents will sign the IJNDB-E “User Agreement for Participation in an Electronic Communications System” before using or accessing any district computer or network resources.

III. User-specific provisions

A .All Users agree to not

1. Access and/or transmit material in violation of any U.S. or Commonwealth law, including copyrighted material, over the District network.
2. Access, download, display, transmit, produce, generate, copy or propagate any material that is obscene or pornographic material; advocates illegal acts; contains ethnic slurs, or racial epithets; or discriminates on the basis of gender, national origin, sexual orientation, race, religion, ethnicity, handicap or age.
3. Degrade, damage or disrupt equipment or system performance.
4. Gain unauthorized access to network resources.
5. Permit or authorize any other person to use their name or login password.

6. Use an account of any other person or vandalize another user's data.
7. Waste electronic storage space by saving unnecessary files or programs. This includes personal video, music, and image files.
8. Download, install, load or use programs without permission from the technology department.
9. Use the Internet for personal commercial purposes or for political lobbying.
10. Harass or annoy any other party with obscene, libelous, threatening or anonymous messages, objectionable information, images or language.
11. Forward e-mail messages of broad interest-including virus alerts and jokes-to the entire school community.
12. Knowingly make use of pirated software or violate software- licensing agreements.
13. Engage in the practice of "hacking" or knowingly engage in any other illegal activity with using the network.

B. Students

1. Students may access the Internet only with adult supervision, and must notify a teacher or technology personnel immediately if they come across inappropriate content.
2. Students may not use the Internet to give out personal information (such as a home address, telephone number, or picture) about themselves or other students. Exceptions to this policy will be made exclusively by District administration.
3. Student use of electronic resources is restricted to teacher approved projects and research.
4. Students found to be using any electronic communications device in any way that violates student code of conduct expectations, including but not limited to bullying, harassing, or civil rights violating behaviors, will be subject to disciplinary action and the device shall be confiscated and not returned until a parent conference is held. This includes violations while off school property and after school hours. Students violating this rule may be disallowed from carrying any personal communication device following the incident unless it can be established by the building Principal that such a device is necessary for a bona fide health or safety emergency.

IV. Electronic communications include, but are not limited to E-mail

School and district resources for electronic communication shall be used for educational purposes. Students, short-term subs, and guest teachers are not issued email accounts. Incidental and occasional personal use of electronic mail may occur when such use does not generate a direct cost for the district, but such messages will be treated no differently from other messages on the network.

A. Prohibited electronic communications include, but are not limited to:

1. Use of electronic communications to send copies of documents in violation of copyright laws.
2. Use of electronic communication to send messages or information restricted by laws and regulations.
3. Use of electronic communications to intimidate others or to interfere with the ability of others to conduct school/district business.
4. Constructing electronic communications so they appear to be from someone else.
5. Forwarding of chain letters.
6. Use of inappropriate, offensive, foul or abusive language.
7. Marketing of any products or services for profit.
8. Solicitation of events and causes not directly affiliated with the district.

V.Text Messaging

1. Students are not permitted to access text messaging on any device during class time, unless directed by a teacher for educational purposes.
2. Staff will follow the policies outlined in the “GMRSD Social Media Policy” when engaging in text message communications with any students or staff.

VI.Software policy

Software licensing will be adhered to without exception.

A. Computer workstation and laptop software

1. Software is not to be installed on a district owned computer by anyone except the technology personnel. Specific software can be made available upon request to the Technology Department.

B. Tablet and mobile device software

1. Only district assigned email and software (iTunes) accounts are to be used on devices issued to or used by students.

2. Any application installed on a district owned device that may be accessed by a student must first be approved by a school administrator.
3. Application requests are made by filling out an “iPad Application Request Form” and submitting it to their building Principal. Download - http://www.gmrsd.org/forms/ipad_app_request.pdf

VII.Network Policy

A. Wired Network
1. Only District owned electronic devices are permitted to connect to the District’s wired network.
2. Personal electronic devices are never permitted to connect to the District’s wired computer network without prior authorization of the Technology Department.

B. Wireless Network Policy (WiFi)
1. Student’s personal devices are not allowed to connect to any District wireless network.
2. Staff owned electronic devices are only allowed to connect to the “gmsd-guest” network.
3. Staff is never to disseminate wireless network passwords.

VIII. Social Media and Web Page Policy
1. Staff will adhere to the “GMRSD Electronic Communication and Social Media Policy”.

IX. Public Records Law and Copyright Protection
The Attorney General of the Commonwealth of Massachusetts has determined that any document created or received by a public employee in his or her capacity as such is subject to retention and perhaps disclosure under the public records law.
A. Except for inappropriate postings, staff shall not delete any message posted on a social media site, webpage, blog, homework page, etc. In cases of inappropriate postings, the posting is to be copied and sent to an administrator using your district email account. The posting is then to be deleted from the site.
B. Staff shall save all direct messages and communications conveyed through district affiliated social media sites. All email sent or received by district email accounts is archived for a minimum of 7 years.
C. Staff shall comply with applicable copyright laws when posting information produced by another person or entity and shall cite all third-party sources of information posted or shared.

January 28, 2014