

## **EMPLOYEE USE OF INFORMATION TECHNOLOGY**

### **INTRODUCTION**

The Merrimack School District recognizes that information technology is a tool that, when responsibly applied, enhances the classroom experience and extends learning beyond the school walls. With information technology saturating nearly every aspect of our lives, it is incumbent upon the District to provide the members of the school community with an understanding of what the District considers to be appropriate use of information technology by employees. Substitutes, volunteers, consultants and guests are also expected to uphold the responsibilities outlined in this policy.

While this policy is intended to provide guidelines for responsible use of information technology, it cannot cover all possible uses. When using District-provided information technology, employees must demonstrate the same level of professionalism and appropriate behavior as they would in using any other District resource. Employees must also recognize that their personal online conduct, whether or not it utilizes District provided Information Technology, may have an impact on their role as an employee of the District and the same level of professionalism must be applied to such uses.

### **DEFINITIONS**

1. District Information Technology – District Information Technology includes all Merrimack School District computers, computing devices, software, servers, desk phones, cell phones, and network and internet connectivity.
2. District Business - District Business includes any matter pertaining to student(s), staff, policies, procedures, contracts, negotiations, District finances, curricular and co-curricular activities, student activities, school outings or trips, or any other matters involving District operations.

### **GUIDELINES FOR RESPONSIBLE USE OF DISTRICT INFORMATION TECHNOLOGY**

The following Guidelines are intended to establish the parameters of Responsible Use of Information Technology in the District. In addition, employees are expected to comply with all rules and policies of the school and the Merrimack School District, including the Code of Conduct, set forth below, in all District-related communication and online activity.

1. Comply with all applicable laws and regulations, such as copyright laws and “fair-use” guidelines.
2. Whenever possible, use District-provided communication systems (eg; School World, District e-mail) when conducting District Business, particularly business involving students, personnel, or financial information. Employees wishing to use their own communication systems (eg. Social Media) when conducting District Business, **must** obtain prior approval by the building administrator or his/her designee.

3. Recognize that District Information Technology is intended to support the education mission of the District. Given the limited nature of some technology resources (such as bandwidth and computer availability), incidental personal use of District Information Technology shall not incur cost to the District (i.e. printing) and must not interfere with job responsibilities or with the efficient operation of the Merrimack School District.
4. Conduct all District-related communication in a respectful, appropriate and professional manner at all times. This extends to all communication, whether electronic or in print, and all representation of the District, regardless of venue or occasion.
5. Protect student privacy in all communications. Any time that student information is included in a written or electronic communication, the communication may be considered a student record subject to the Federal Education Record Protection Act. *[Please consult **Digital Communication Guidelines for Professional and Support Staff**].*
6. Follow District policies and procedures when creating or posting materials on District-sponsored websites. *[Please consult **Guidelines for Staff Web Sites and Online Digital Content**]* Websites created by staff for school-related purposes must be linked to the District website. Any external links provided on a District-sponsored web site or communication must be checked for content and appropriateness prior to being included in the site or communication and must contain a disclaimer stating that any links to external websites are provided for convenience and the District does not endorse the site or have any responsibility for the content of the external site.
7. Understand privacy settings, how systems will display or share posted information, and the extent to which any postings can be forwarded, reposted or altered without your knowledge.
8. Follow the procedure outlined in the ***Criteria for Publication of School-Related Information on the Internet*** when using any student likeness, work, or information in a District-sponsored web site or communication.
9. Request technical assistance and report misuse, abuse, or problems with District Information Technology, or related District equipment, to the appropriate technology staff immediately upon discovery.
10. Help maintain the integrity of District technology by not engaging in the following activities, or those of a similar nature, and by reporting any knowledge of such activity by others:
  - a. using or attempting to use others' credentials, identities, passwords or logins
  - b. hacking
  - c. adding unauthorized software to district systems
  - d. disabling or attempting to disable the District's filtering/blocking technology
  - e. deleting, erasing or concealing any information or file stored on a District computer or system which contains or relates to District Business or relates to any student, other than in the normal course of performing the employee's duties or in accordance with the District's record retention and destruction policies
  - f. intentionally or maliciously damaging District computers or technology devices or causing disruption or interruption to District network internet systems

**CODE OF CONDUCT/PROHIBITED ACTIVITIES**

All employees using District Information Technology are responsible for complying with the following rules of conduct and must understand that **the ability to access is not permission to access.**

1. Do not use District Information Technology to find, view, or distribute threatening, harassing, discriminatory, defamatory, sexually explicit, obscene, pornographic, violent or otherwise inappropriate material.
2. Do not use District Information Technology for private financial or commercial purposes or as a forum for communicating the views of or for soliciting membership, support, or contributions in or to any non-District sponsored or non-District recognized group or organization.
3. Do not use District Information Technology to communicate with students or minors on non-school related matters.
4. Do not access or attempt to access unauthorized websites or access or attempt to access files, folders, or other systems of others either deliberately or accidentally (such as when a user does not logout of a computer or application), unless authorized to do so.

**CAUTIONS TO USERS OF DISTRICT INFORMATION TECHNOLOGY**

1. District Information Technology is the property of the District and remains under the control, custody and supervision of the District. Information contained on or transmitted through the District server or network is not private and the District reserves the right to monitor and inspect all employee use of District Information Technology, even if conducted after school hours and off of school premises.
2. Any electronic communication pertaining to District Business is subject to this policy and may be considered a public record, regardless of the device or network used. Personal computers and other technology devices used for District Business may be subject to inspection by the District.
3. The use of Information Technology in the District is a right that comes with responsibility. Inappropriate use may result in the curtailment of that right. District administrators or their designees shall make all decisions regarding whether or not a user has violated these guidelines and may deny, revoke, or suspend access at any time.
4. Accessing obscene, pornographic, or other material harmful to minors is strictly prohibited. While the District filters content as required by the Children's Internet Protection Act [Public Law 106-554], filtering is inherently imperfect and cannot substitute for sound professional judgment when using Information Technology in the District.
5. Any employee who fails to comply with the Guidelines for Responsible Use or violates the Code of Conduct set forth in this policy will be subject to disciplinary action, up to and including termination of employment, and depending on the nature of the violation may also be referred to law enforcement.
6. The Merrimack School District is not responsible for any loss of data due to circumstances beyond its control or from users' errors or omissions. The District is not responsible for the upkeep or maintenance of personal computers or other technology devices, unless arranged in advance with administration or library media and technology staff.

**EMPLOYEE USE OF SOCIAL MEDIA**

The Merrimack School District recognizes that social media, in all its forms and iterations (e.g. blogs, MS 365, Facebook, Twitter, Tumblr, YouTube, etc.), can be an important tool of education and communication. As such, its availability as a resource is understood as just one component of the district's overall educational mission. However, any use of social media by a district employee for school related purposes must be consistent with the professional expectations set forth in this policy. Toward this end, educators must:

- teach students about appropriate online behavior, including proper interactions with others on social networking web sites
- build awareness of cyber bullying,
- proactively supervise student use of information technology
- enforce District policies regarding student use of information technology.

**Employees who choose to use social media for communicating with students about school-related matters must adhere to the following:**

- Secure approval from building administrator or his/her designee prior to using social media to communicate with students.
- Setup a non-personal account on whatever social media site is being used
  - Employees must provide site and login credentials to building administrator or designee
- Maintain professional boundaries with students
- Not post to Social Media images, videos or any form of student likeness or identification without the express prior written permission of parents.

**Employees who use social media for personal purposes must:**

- Not connect with students on social media sites using personal accounts.
- Not discuss a particular student(s), staff or other confidential District Business.
- Express only one's own personal opinions.
  - If your communication relates to the District, the employee must disclose the fact that they are an employee of the District and must include a disclaimer such as "The postings on this site are my own and do not necessarily reflect the views of the District."
- Not use their District email address on social media sites, unless it is related to District Business.
- Not post material that could be considered malicious, obscene, threatening, harassing or disparaging towards a co-worker, student or parent.
  - Remember, you will be responsible for whatever you post.
  - Remember that what you post on the internet may be viewed by students and parents. Therefore, it is important to portray a professional image at all times.

Legal Reference:

RSA 194:3-d, School District Computer Networks  
RSA 91Section 91-A:4 Minutes and Records Available for Public Inspection.  
Pub. L. No. 106-554, Children's Internet Protection Act  
Federal Educational Record Protection Act

Resources

[Guidelines for Staff Web Sites and Online Digital Content](#)  
[Digital Communication Guidelines for Professional and Support Staff](#)  
[Digital Communication Guidelines for Parents and Community](#)  
[Criteria for Publication of School-Related Information on the Internet](#)

1<sup>st</sup> Reading: February 18, 2013  
2<sup>nd</sup> Review: April 1, 2013  
3<sup>rd</sup> Review: May 20, 2013  
4<sup>th</sup> Review: June 17, 2013  
5<sup>th</sup> Review: July 15, 2013  
Adoption: July 15, 2013