

## RESPONSIBLE USE POLICY

### 1. Purpose

The Mansfield Public Schools provides computing resources and Internet access to support the District's educational, instructional, administrative and operational activities. The use of these resources is a privilege that is extended to members of the Mansfield Public Schools community. As a user of these services and facilities, you have access to valuable district resources, to sensitive data, and to internal and external networks. This policy explains the District's expectations for using these resources responsibly, ethically, productively, and legally.

### 2. Scope

This policy applies to all users of computing resources owned or managed by the Mansfield Public Schools. Individuals covered by this policy include but are not limited to employees, students, members of the School Committee, volunteers, guests, and external individuals and organizations accessing the District's technology, network, and data systems whether on school grounds or in another location.

Computing resources include all District-owned, licensed, or managed hardware and software or any use of the district network via a physical, wireless, or remote connection, regardless of the ownership of the computer or device connected to the network.

#### 2.1 Consequences

If a user violates this policy, the District will take appropriate action, which may include restriction and loss of network privileges, payments for damages or repairs, and discipline under appropriate District policies up to and including suspension or expulsion, termination of employment, and referral to legal authorities. Users may also be held personally liable under applicable state and federal civil or criminal laws. Employee discipline procedures will be in accordance with the terms of applicable collective bargaining agreements.

### Definitions

**The Massachusetts Public Record Law** is a law that gives the public the right to request access to information from a Massachusetts governmental agency. The **Freedom of Information Act (FOIA)** is a law that gives the public access to information from the federal government. A public records request can be made to the Mansfield Public Schools for electronic documents/communications stored or transmitted through district systems unless that information is exempted from disclosure by law.

**Family Educational Rights and Privacy Act (FERPA)** protects the privacy of student education records. Personal information stored or transmitted by the Mansfield Public Schools must abide by FERPA. The Mansfield Public Schools also is required to protect the *Mansfield Public Schools*

## RESPONSIBLE USE POLICY

confidentiality, integrity, and security of student records under MA general law and Board of Education regulations.

**Children's Internet Protection Act (CIPA)** requires schools that receive federal funding through the E-Rate program to protect students from content deemed harmful or inappropriate. The Mansfield Public Schools is required to filter Internet access for inappropriate content, monitor the Internet usage of minors, and provide education to students and staff on safe and appropriate online behavior.

**Children's Online Privacy Protection Act (COPPA)** imposes certain requirements on operators of websites or online services directed to children under 13 years of age, and on operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age. The primary goal of COPPA is to place parents in control over what information is collected from their children online.

**The Health Insurance Portability and Privacy Act (HIPAA)** establishes national standards to protect the privacy of personal health information and medical records, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization.

### 3. Policy

#### 3.1 Responsible Use – General Principles

We expect students, staff, and guests to conduct business in accordance with the letter, spirit, and intent of all relevant laws and not to do anything that is illegal, dishonest, or unethical. By using Mansfield Public Schools Internet systems and devices, the user agrees to follow all District policies, regulations, and guidelines and state and federal law. Students are expected to and employees are required to report misuse or breach of protocols to appropriate district personnel.

- All computing devices, software, applications, data, and network and internet connectivity furnished to employees are property of the Mansfield Public Schools and are intended for educational or business use that is consistent with the mission of the District.
- We expect users to exercise good judgment in the use of these resources and to have the highest standards of conduct and personal integrity. Users are responsible for knowing and complying with the regulations and policies and laws that apply to the appropriate use of District technology and resources. If you use good judgment and follow high ethical principles, you will make the right decisions. If you are not sure if an action is legal, ethical, or proper, you should discuss the matter openly with your teacher or supervisor.

## RESPONSIBLE USE POLICY

- All federal, state, and local laws and District policies and behavior guidelines that cover student and employee conduct on school premises and at school-related activities similarly apply to the online environment in those same venues.
- While District computing resources are intended for job- and education-related activities, we permit brief personal use within reasonable limits.
- Any use of the District's computing resources in ways that disrupt the school environment, contributes to creating a harassing workplace, or creates a legal risk to the District is prohibited.
- Using computing resources to create or disseminate content that could be considered discriminatory, obscene, threatening, harassing, libelous, retaliatory, or intimidating to any other person is not allowed and could lead to disciplinary action by the District as well as legal action by those who are the recipient of these actions.
- District computing resources may not be used to post or send items with sexually obscene content or images exhibiting or advocating the illegal use of drugs or alcohol is prohibited.
- District computing resources may not be used to solicit and/or promote others for commercial ventures or personal economic gain, for religious or political causes, for outside organizations, or other non-District matters.
- Users are expected to conserve and fairly share District resources through the proper and considerate use of printers, server space, video or audio streaming, and network bandwidth.
- All Internet data that is composed, transmitted, or received via our devices and network is considered the property of the Mansfield Public Schools and part of our records and may be subject to disclosure to law enforcement or other third parties.
- Nothing in this policy will be read to limit an individual's constitutional rights to freedom of speech or expression or to restrict an employee's ability to engage in concerted, protected activity with fellow employees regarding the terms and conditions of their employment. Notwithstanding this, when staff members speak through social media on matters concerning their work, they should be aware that they are speaking as employees of the Mansfield Public Schools.

### 3.1.2 Student and Staff Records Privacy

The District has a legal and moral obligation to protect the personal data of students, families, and staff. Personal information for students/families and staff must be stored and transmitted using approved practices and systems.

The Mansfield Public Schools complies with the Children's Internet Protection Act (CIPA), the Children's Online Privacy Protection Act (COPPA), and the Family Educational Rights and Privacy Act (FERPA), as well as state law and regulations concerning the security and *Mansfield Public Schools*

## **RESPONSIBLE USE POLICY**

confidentiality of employee information and to protect against unauthorized access to or use of such information.

Employees who use third-party software/applications/cloud-storage services to facilitate student learning must have approval in writing from the building Principal. The Director of Technology or designee will ensure such products are CIPA- and/or FERPA-compliant before approval is given.

### **3.1.3 Copyright and Intellectual Property**

The Mansfield Public Schools does not allow the unauthorized use, installation, copying, or distribution of copyrighted, trademarked, or patented software or material (including music, videos, games, images, text and other media) or any other unauthorized software or material on the Internet.

As a responsible user of the District's computing and network resources, you must abide by all applicable copyright laws and licenses and observe copyright laws. As a general rule, if you did not create the material, you do not own the rights to it, or if you have not received authorization for its use, you may not put the material on the Internet, including works created by students and staff.

### **3.1.4 Social Networking, Electronic Messaging, and Phone Usage**

The Mansfield Public Schools encourages the appropriate use of online communication, including social media, to increase student and staff learning, parent and community engagement, and operational efficiency.

When using online tools, members of the Mansfield Public Schools community when acting as representatives or employees of the Mansfield Public Schools will use appropriate behavior when the communication impacts or is likely to impact the classroom or working environment in the Mansfield Public Schools.

- Employees should model and actively practice positive digital citizenship and help students use new technologies in a meaningful, safe, and responsible way. Employees utilizing social media with students are expected to educate students about digital citizenship, which includes appropriate and safe online behavior, interacting with individuals on social networking websites, and cyber-bullying awareness.
- Employee activities on district-affiliated social media or social networking websites should not reflect negatively on students, staff, or the District. Employees should respect the District's good name in all electronic interactions and act in ways that will earn the continued trust and confidence of the public.

***Mansfield Public Schools***

## **RESPONSIBLE USE POLICY**

- Employees who use internal or external social media (blogs, Twitter, etc.) are expected to maintain professionalism at all times. This includes refraining from discussing confidential information and/or discussing specific students. Information that can be traced back to a specific student or could allow a student to be publicly identified should not be posted on any social media sites.
- Employees and students in grades 3 – 12 are provided with district email accounts and online tools to improve the efficiency and effectiveness of communication, both within the organization and with the broader community. Employee communication should be consistent with professional practices used for all correspondence.
- All communication sent by an employee using district property or regarding district business could be subjected to public access requests. Users need to be aware that data and other material/files maintained on the school district systems may be subject to review, disclosure, or discovery.
- Employee use of personal email accounts and communication tools to conduct school business is strongly discouraged and may open an individual's personal account to be subject to public records inquiries under state and federal law.
- Employees may set up a district approved third-party site to facilitate student learning.
- Unapproved third-party sites, including social media accounts, require written permission of the building principal.
- Employees are prohibited from exchanging personal telephone contact information with current students of any age without explicit written permission of the Principal. The Principal may authorize such exchanges in situations where student safety or operational efficiency would be improved by communication by telephone.
- Coaches or club/activity advisors are prohibited from exchanging personal telephone or email contact information with student team or club/activity members without prior approval of the Principal or his/her designee. All electronic or telephone contact by coaches and club/activity advisors with students will be sent to two or more team members, except for messages that would compromise confidential information, such as medical or academic privacy matters. Messages from coaches and club/activity advisors sent to individual students will be copied to the Principal or his/her designee.

### **3.1.5 System Security**

Users should not share their password or use another person's password, another user account, access a file, or retrieve any stored communication without authorization from the building Principal or Central Office.

## **RESPONSIBLE USE POLICY**

Hacking or attempting to access computer systems without authorization, vandalism (including the uploading or creation of computer viruses, worms, or malware), fraud, phishing, spamming, and/or unauthorized tampering with computer systems is prohibited and may result in district disciplinary action as well as legal action.

### **3.2 Monitoring**

All computer equipment, services, or technology that we furnish are the property of the Mansfield Public Schools, and users should have no expectation of privacy. We reserve the right to monitor local network and Internet traffic, including information sent or received through our online connections or stored on our computer systems for any reason, including but not limited to ensuring quality control and investigate system problems, ensuring student and employee safety and district security, or as may be necessary, ensuring that the District is not subject to claims of misconduct.

The Superintendent or designee will approve access to files on District-owned equipment or information only when there is a valid reason to access those files. Authority to access user files can only come from the Director of Technology in conjunction with requests and/or approvals from the Superintendent or designee. External law enforcement agencies may request access to files through valid subpoenas and other legally binding requests. The District's legal counsel must review all such requests. Information obtained in this manner can be admissible in legal proceedings or in a District discipline hearing.

### **3.3 User Compliance & District Liability**

You will not be permitted to use school-based technology resources without a signed Responsible Use Policy or guest-user agreement. Signed student and employee RUPs will remain on file at each school.

When you use District computing services and accept any District-issued computing accounts, you agree to comply with this policy and all other computing-related policies. You have the responsibility to keep up-to-date on changes in the District computing environment via District electronic and print publication mechanisms, and to adapt to those changes as necessary.

The Mansfield Public Schools and its representatives do not encourage or endorse access to inappropriate materials or undesirable persons. The Mansfield Public Schools makes no warranties of any kind, whether expressed or implied, for the technology-related services it provides and will not be responsible for any damages resulting from delays or service interruptions caused by its own negligence or the user's errors or omissions information obtained via the Internet is at the user's own risk. The Mansfield Public Schools specifically denies any responsibility for the accuracy or quality of information obtained through its computer services.

***Mansfield Public Schools***

## RESPONSIBLE USE POLICY

### 4. Policy Review and Notice

The Director of Technology and Superintendent or designee will review this policy annually.

District administration will provide written notice annually to staff, students and parents/guardians of the responsible use policy. Such notification will include, but not be limited to, employee handbooks, student/parent handbooks, and the District website.

Adopted: June 13, 2016

LEGAL REFS: M.G.L 66:10 Massachusetts Public Record Law  
M.G.L. 71:34D Student Records; Regulations  
M.G.L 71:37H Publication of School Committee Rules and Regulations  
Relative to the Conduct of Teachers and Students  
Freedom of Information Act (FOIA)  
Family Educational Rights and Privacy Act (FERPA)  
Children's Internet Protection Act (CIPA)  
Children's Online Privacy Protection Act (COPPA)  
Health Insurance Portability and Privacy Act (HIPAA)

OTHER REFS: Boston Public Schools Acceptable Use Policy  
Duxbury Public Schools Acceptable Use Policy  
Foxborough Public Schools Acceptable Use Policy  
Sharon Public Schools Acceptable Use Policy  
High Tech High Acceptable Use Policy  
Massachusetts Association of School Committees (MASC)

CROSS REFS: AC, Nondiscrimination  
ACAB, Sexual Harassment  
JBA, Student-to-Student Harassment  
JIC, Student Discipline  
JICFA, Prohibition of Hazing  
JICFB, Bullying Prevention and Intervention  
JICFC, Teen Dating Violence  
JK, Student Conduct  
JRA, Student Records