File: IJNDB-R

ACCEPTABLE USE POLICY - TECHNOLOGY

Administrative Procedures for Implementation

1. Commercial use of the system/network is prohibited.
2. The district will provide training to users in the proper use of the system/network.
3. The district will provide each user with copies of the Acceptable Use Policy and Procedures.
4. Copyrighted software or data shall not be placed on the district system/network without permission from the holder of the copyright and the system administrator.
5. Access will be granted to employees with a signed access agreement and permission of their supervisor.
6. Access will be granted to students with a signed access agreement and permission of the building administrator or designee(s).
7. Account names will be recorded on access agreements and kept on file at the building level.
8. Initial passwords provided by the network administrator should be set to expire on login.
9. Passwords shall be changed every 15 days and all passwords shall be expired at the end of each school year.
10. Passwords are confidential. All passwords shall be protected by the user and not shared or displayed.
11. Students completing required course work will have first priority for after hours use of equipment.
12. Principals or their designee will be responsible for disseminating and enforcing policies and procedures in the building(s) under their control.
13. Principals or their designee will ensure that all users complete and sign an agreement to abide by policies and procedures regarding use of the system/network. All such agreements are to maintained at the building level.
14. Principals or their designee will ensure that training is provided to users on appropriate use of electronic resources.
15. Principals or their designee shall be authorized to monitor or examine all system activities, including electronic mail transmissions, as deemed appropriate to ensure proper use of electronic resources.
16. Principals or their designee shall be responsible for establishing appropriate retention and backup schedules.
17. Principals or their designee shall be responsible for establishing disk usage limitations, if needed.
18. Individual users shall, at all times, be responsible for the proper use of accounts issued in their name.
19. The system/network may not be used for illegal purposes, in support of illegal activities, or for any activity prohibited by district policy.

20. System users shall not use another user's account.
21. System users should purge electronic information according to district retention guidelines.
22. System users may redistribute copyrighted material only with the written permission of the copyright holder or designee. Such permission must be specified in the document or in accordance with applicable copyright laws, district policy, and administrative procedures.
23. System administrators may upload/download public domain programs to the system/network. System administrators are responsible for determining if a program is in the public domain.
24. Any malicious attempt to harm or destroy equipment, materials, data, or programs is prohibited.
25. Deliberate attempts to degrade or disrupt system performance may be viewed as violations of district policy and/or as criminal activity under applicable state and federal laws. This includes, but is not limited to, the uploading or creation of computer viruses.
26. Vandalism will result in the cancellation of system privileges and will require restitution for costs associated with hardware, software, and system restoration.
27. Forgery or attempted forgery is prohibited.
28. Attempts to read, delete, copy, or modify the electronic mail of other users or to interfere with the ability of other users to send/receive electronic mail is prohibited.
29. Use appropriate language; swearing, vulgarity, ethnic or racial slurs, and other inflammatory language is prohibited.
30. Pretending to be someone else when sending/receiving message is prohibited.
31. Transmitting or viewing obscene material is prohibited.
32. Revealing personal information (addresses, phone numbers, etc.) is prohibited.
33. The district will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the district's system/network.

A user who violates district policy or administrative procedures will be subject to suspension or termination of system/network privileges and will be subject to appropriate disciplinary action and/or prosecution.

File: IJNDB-R

Webster Public Schools Acceptable Use Policy

1. Purpose

The Webster Public Schools provides technology resources 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 Webster 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 in a productive, responsible, ethical,and legal manner.

2. Scope

This policy applies to all users of technology resources owned or managed by the Webster Public Schools. Individuals covered by this policy include but are not limited to employees, members of the School Committee, volunteers, guests, and external individuals and organizations accessing the District's technology resources 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 technology privileges, payments for damages or repairs, and discipline under appropriate District policies up to and including suspension, 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. Users are encouraged to report misuse or violations of this policy to appropriate personnel, including building administrators and the Manager of Technology, Learning, and Innovation.

2.2 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 Webster Public Schools for electronic documents/communications stored or transmitted through district systems unless that information is specifically 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 Webster Public Schools must abide by FERPA.

The Webster Public Schools also are required to protect the confidentiality, integrity, and security of student records under MA 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 Webster Public Schools are 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.

3. Policy

3.1 Responsible Use – General Principles

We expect users to conduct business in accordance with the letter, spirit, and intent of all relevant laws and to not do anything that is illegal, dishonest, or unethical. By using Webster Public Schools technology resources the user agrees to follow all District policies, regulations, and guidelines, as well as state and federal laws. Employees are required to report misuse or breach of protocols to appropriate District personnel.

- All technology resources furnished to employees are property of the Webster 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 are not sure if an action is legal, ethical, or appropriate, you should discuss the matter with your mentor or supervisor.

- Users are prohibited from using technology for inappropriate purposes including but not limited to the following: playing games, gambling, downloading unapproved files, viewing or processing inappropriate text files or pictures (e.g., sites dealing with antisocial behavior, pornography, obscenity, profanity, discrimination or files which may be dangerous to the integrity of the network).

- 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.

- District computing resources are intended for job and education related activities. We permit brief personal use, or use for reasons permitted by state law, within reasonable limits as long as such activities don't interfere with employee work tasks.

- Any use of the District's computing resources in ways that disrupt the school environment, is inappropriate and/or unprofessional, contributes to creating a harassing workplace, or creates a legal risk to the District is prohibited.

- Access to view, edit, or share personal data of students and employees must be by authorized individuals only, who must abide by federal and state laws and regulations, including ensuring privacy. When educational records, personal information, or other private data is transmitted or shared electronically, staff are expected to protect the privacy of data. Staff must also ensure records are sent to individuals with a right to said records and ensure that only the intended recipient(s) are able to access the data.

- Using computing resources to create or disseminate content that could be considered discriminatory, obscene, threatening, harassing, defamatory, 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 access, post, or send items with sexually obscene content. Similarly, images exhibiting or advocating the illegal use of drugs or alcohol is prohibited.

- Users must not photograph or make audio/video recordings without the consent of those being recorded and/or permission granted by a parent/guardian of those being recorded. This shall not apply to "directory information" or other fair use authorized under federal or state student records law.

- 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.

- All activity that is composed, transmitted, or received via our technology resources is considered the property of the Webster Public Schools and part of the District's 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 Webster Public Schools.

3.1.2 Student and Staff Records Privacy

The District has a legal 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 Webster 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 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*** verify that the District has approved the use of said resources. Approved resources are vetted for compliance with all relevant student data privacy laws and regulations.

3.1.3 Copyright and Intellectual Property

The Webster 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 Online Communication

The Webster 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 Webster Public Schools community when acting as representatives or employees of the Webster Public Schools will use appropriate behavior when the communication impacts or is likely to impact the classroom or working environment in the Webster Public Schools.

- Employees should model and actively practice positive digital citizenship and help students use new technologies in a safe, and responsible way. Employees utilizing online communication platforms 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 who use internal or external social media sites are expected to maintain professionalism at all times. This includes refraining from discussing confidential information and/or discussing specific students. Content 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 are provided with online tools to support teaching and learning and to improve the efficiency and effectiveness of communication, both within the organization and with the broader community. Staff and students in grades K through 12 are also provided with District email accounts. Employee communication over email should be consistent with professional practices used for all correspondence.

- All communication sent by an employee using District resources or regarding District business could be subjected to public record requests. Users need to be aware that emails, chats, data and other material/files maintained on the District's systems or the cloud may be subject to review, disclosure, or discovery.

- Employee use of personal email accounts and communication tools to conduct school business is not allowed. Personal email accounts should not be accessed on District Owned hardware.

- Before using an online resource, staff are required to verify it has been approved for use. Approval indicates that the resource meets Webster's standard for student data privacy and aligns with Webster's curriculum and instruction standards. This can be done via the Curriculum and I.T. Departments, as well as asking your school's leadership and/or administration.

- Employees are prohibited from exchanging personal contact information and/or friending/following on social media with current students of any age without explicit written permission of the Principal.

- Coaches or club/activity advisors should refrain from exchanging personal contact information with student team, club/activity members, or their parents/guardians. Rather, coaches and advisors shall use District approved communication platforms for the purpose of communicating with these individuals. It is strongly recommended that 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.

3.1.5 System Security

Users should not share their password or use another person's password. Users should not access another user's account, file, or retrieve any stored communication without authorization from the Superintendent or Business Manager.

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. Users may not use proxy or VPN services to negate or otherwise bypass the District's filtering and monitoring of content.

Users must take responsible measures to prevent a device from being lost or stolen. In the event an electronic device is lost or stolen, the user is required to notify appropriate school staff immediately. The District will attempt to recover the lost property and ensure the security of any information contained on the device.

3.2 Monitoring

All technologies that we furnish are the property of the Webster 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, ensuring appropriate use, 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 Manager of Information 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 will 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

All staff are required to agree to the terms of this Acceptable Use Policy during the new-hire onboarding process or when changes to this policy are adopted by the School Committee.

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 adhere to those changes.

The Webster Public Schools and its representatives do not encourage or endorse access to inappropriate materials or persons. The Webster 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 Webster Public Schools specifically denies any responsibility for the accuracy or quality of information obtained through its computer services.

The Webster Public Schools 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 Webster Public Schools shall not be responsible for ensuring the accuracy or usability of any information found on external networks.

It is the responsibility of the employee to check their school email account daily. Important information is delivered through the school district email system.

4. Policy Review and Notice

The Manager of Information Technology or designee will review this policy annually.

District administration will provide written notice upon adoption of changes to staff regarding this policy. Such notification will include, but not be limited to, employee handbooks and the District website.

Revised: September 17, 2025
Adopted:

LEGAL REFS: M.G.L. 66 §10: Massachusetts Public Record Law; M.G.L. 71 §34D and 603 CMR 23.00: Mass. Student Records Law and 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)

OTHER REFS: Westwood Public Schools Acceptable Use Policy, Chelmsford Public Schools Acceptable Use Policy, East Longmeadow Schools Acceptable Use Policy and Massachusetts Association of School Committees (MASC)

First Reading:	September 23, 2025
Second Reading:	October 14, 2025
Third and Final Reading:	October 28, 2025