

West Bridgewater Public Schools
West Bridgewater, Massachusetts

**Administrative Procedures:
Use of School Department's Computer System**

1. The district will provide each user with two (2) copies of the Acceptable Internet Use Policy and Procedures. One copy is to be signed and returned to the principal for inclusion in the employee's personnel file.
2. The district will provide training to users in the proper use of the computer network. All employees who will be using the School Department's computer system are expected to familiarize themselves with it. The School Department will provide no cost training for employees.
3. Access to the School Department's computer system will be granted to employees only after they sign the Internet policy and return it to their building principal.
4. Each building principal or their designee will, from time-to-time, issue a roster of approved computer users. Employees should not permit students whose names do not appear on the roster of approved computer users to use the school department's computer system. Access will be granted to students with a signed Internet Use Policy and permission of building administrator or designee(s).
5. Account names will be recorded on access agreements and receipt forms and kept on file at the building level.
6. Passwords shall be issued at the beginning of each school year and shall expire at the end of each school year.
7. Passwords are confidential. All passwords shall be protected by the user and neither shared, nor displayed.
8. Students completing required course work will have priority over other students for after-hours use of equipment.
9. Principals or their designee will be responsible for disseminating and enforcing policies and procedures in the building(s) under their control.
10. Principals or their designee will ensure that all users complete and sign an agreement to abide by policies and procedures regarding use of the computer network. All such agreements are to be maintained at the building level.
11. 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 mail resources. Whenever an employee's system activity is

monitored or examined by school personnel, he/she shall be notified in writing within 48 hours.

12. Principals or their designee shall be responsible for establishing appropriate retention and backup schedules. Before any information is deleted from the school department's computer system by anyone using the system, they should insure that it is permissible to delete pursuant to the state's public records' law.
13. Principals or their designee shall be responsible for establishing disk usage limitations, if needed.
14. Individual users shall, at all times, be responsible for their use of accounts issued in their name.
15. System users should purge electronic information according to district retention guidelines, which must be in compliance with the state's public records laws.
16. System users may redistribute copyrighted material only with 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 administration procedures.
17. System administrator may upload/download public domain programs to the computer network. System administrators are responsible for determining if a program is in the public domain.
18. Commercial use of the computer network is prohibited.
19. Copyrighted software or data shall not be distributed or placed on the district computer network without permission from the holder of the copyright and the system administrator.
20. The computer network may not be used for illegal purposes, in support of illegal activities, for any activity prohibited by district policy, or in any way that would constitute conduct unbecoming a school department employee.
21. System users shall not use another user's account.
22. Any malicious attempt to harm, improperly access, or destroy equipment, material data, or programs is prohibited.
23. 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.

24. Vandalism will result in the cancellation of system privileges and will require restitution for costs associated with hardware, software, and system restoration.
25. Forgery or attempted forgery is prohibited.
26. 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.
27. Users should always use appropriate language; swearing, vulgarity, ethnic or racial slurs and other inflammatory language is prohibited and may result in disciplinary action including the possibility of dismissal.
28. Pretending to be someone else when sending/receiving messages is prohibited.
29. Transmitting or viewing obscene or vulgar material that lacks educational value is prohibited.
30. Revealing personal information (address, phone numbers, etc.) is prohibited.
31. The district will cooperate fully with local, state, or federal officials in any investigation concerning or related to alleged misuse of the district's computer network.
32. Principals or their designee will support employees in the enforcement of the *Acceptable Internet Use Policy for Students*.

A user who knowingly violates district policy or administrative procedures will be subject to suspension or termination of computer network privileges and may be subject to appropriate disciplinary action, including the possibility of dismissal, and/or prosecution, in the case of an employee, in accordance with the applicable provisions of any governing collective bargaining agreement and/or laws.

Common Sense Rules of the Internet

- Be polite. Do not send abusive messages to others.
- Use appropriate language. Offensive, obscene, defamatory, threatening, discriminating, harassing, or inflammatory language will not be tolerated in any public or private message.
- Adhere to copyright agreements.
- Avoid the deliberate or inadvertent spread of computer viruses.
- Do not use another person's files without permission.

- Do not destroy, abuse, modify, or improperly access the school's hardware or software.
- Do not illegally distribute software.
- Do not place unlawful information on the Internet.
- Do not use the Internet for commercial purposes, product advertising, or political lobbying.
- Do not access, download, store, or print files that are profane or obscene.
- Do not post personal information. This includes yours or another person's home phone number, address, and photographs.
- Keep your password private.
- Do not interfere with, harm or modify the work of other users.
- Do not discuss highly sensitive or confidential school information in e-mail communications.

Remember that it is impossible to guarantee the confidentiality and security of any transmission made on the Internet.