File: IJNDB-R

Holbrook Public Schools

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 are confidential. All passwords shall be protected by the user and not shared or displayed.
10. Principals or their designee will be responsible for disseminating and enforcing policies and procedures in the building(s) under their control.
11. 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 be maintained at the building level.
12. Principals or their designee will ensure that training is provided to users on appropriate use of electronic resources.
13. 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.
14. Principals or their designee shall be responsible for establishing appropriate retention and backup schedules.
15. Principals or their designee shall be responsible for establishing disk usage limitations, if needed.
16. Individual users shall, at all times, be responsible for the proper use of accounts issued in their name.
17. The system/network may not be used for illegal purposes, in support of illegal activities, or for any activity prohibited by District policy.
18. System users shall not use another user's account.
19. System users should purge electronic information according to District retention guidelines.
20. 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.
21. 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.
22. Any malicious attempt to harm or destroy equipment, materials, 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. Use appropriate language; swearing, vulgarity, ethnic or racial slurs, and other inflammatory language is prohibited.
28. Pretending to be someone else when sending/receiving message is prohibited.
29. Transmitting or viewing obscene material is prohibited.
30. Revealing personal information (addresses, phone numbers, etc.) is prohibited.
31. 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.

SOURCE: MASC

Adopted: November 14, 2007