Policy	*Title* **TECHNOLOGY ACCEPTABLE USE POLICY**	*Code* **IJNDB**

HOLLISTON

Purpose

The Holliston Public Schools shall provide access for employees, volunteers, and students to the system/network, including access to external networks, for limited educational purposes. Educational purposes shall be defined as classroom activities, academic research, professional development, and high quality self discovery activities of an educational nature. The purpose of the system/network is to assist in preparing students for success in life and work by providing access to a wide range of information and the ability to communicate with others. The system/network will be used to increase communication (staff, parent, and student), enhance productivity, and assist staff in upgrading existing skills and acquiring new skills through a broader exchange of information. The system/network will also be utilized to provide information to the community, including parents, governmental agencies, and businesses.

Availability

The superintendent or designee shall implement, monitor, and evaluate the district's system/network for instructional and administrative purposes.

Access to the system/network, including external networks, shall be made available to employees and students for instructional and administrative purposes and in accordance with administrative regulations and procedures.

Access to the system/network is a privilege, not a right. All users shall be required to acknowledge receipt and understanding of all administrative regulations and procedures governing use of the system and shall agree in writing or electronically to comply with such regulations and procedures. Noncompliance with applicable regulations and procedures may result in suspension or termination of user privileges and other disciplinary actions consistent with the policies of the Holliston Public Schools. Violations of law may result in criminal prosecution as well as disciplinary action by the Holliston Public Schools.

Acceptable Use

The superintendent or designee shall develop and implement administrative regulations, procedures, and user agreements, consistent with the purposes and mission of the Holliston Public Schools as well as with law and policy governing copyright.

Monitored Use

Electronic mail transmissions, web postings, podcasts, messaging tools, blogs, and other use of emerging technologies by students, employees, and volunteers shall not be considered confidential and may be monitored at any time by designated staff to ensure appropriate use for instructional and administrative purposes.

Liability

The Holliston 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 Holliston Public Schools shall not be responsible for ensuring the accuracy or usability of any information found on external networks. The Holliston Public Schools shall not be liable for any damage to or loss of personal equipment brought in from the outside.

General Policy Provisions

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. Network access will only be granted to employees with a signed (written or electronic) access agreement and permission of their supervisor.
6. Network access will only be granted to students with a signed (written or electronic) access agreement and permission of the building administrator or designee(s).
7. Network access will only be granted to volunteers and visitors with a signed (written or electronic) user agreement and permission of a school or district administrator.
8. All passwords are confidential and shall be protected by the user and not shared or displayed.
9. Students completing required coursework will have first priority for after hours' use of equipment.
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 and emerging technologies.
13. Superintendent or his/her designee shall be authorized to monitor or examine all system activities, including but not limited to electronic mail transmissions, web postings, podcasts, blogs, messaging tools as deemed appropriate to ensure proper use of electronic resources and emerging technologies.
14. Superintendent or his/her designee shall be responsible for establishing appropriate retention and backup schedules.
15. System users should purge electronic information according to district retention guidelines and in compliance with Public Records Laws.
16. Superintendent or his/her designee shall be responsible for establishing disk usage limitations, if needed.
17. Individual users shall, at all times, be responsible for the proper use of accounts issued in their name. Users should not leave their workstations logged in and unattended.
18. The system/network may not be used for illegal purposes, in support of illegal activities, or for any activity prohibited by district policy, including circumventing firewalls and/or accessing forbidden or inappropriate material.
19. System users shall not use another user's account.
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 digital media, including but not limited to electronic mail, websites, data files, digital images, podcasts of other users or to interfere with the ability of other users to send/receive electronic mail or digital media is prohibited.
27. User shall use appropriate language. Swearing, vulgarity, ethnic or racial slurs, and other inflammatory language are prohibited.
28. Pretending to be someone else when sending/receiving messages or posting digital media including but not limited to websites, digital images, and podcasts is prohibited.
29. Transmitting or viewing obscene material is prohibited.
30. Individuals should exercise extreme caution before revealing personal information (address, phone numbers, etc.) on an open internet site.
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 and emerging technologies.
32. 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.
33. Cyber-bullying, as defined in School Committee Policy JICFB, using either school-owned or non-school-owned equipment is strictly prohibited.

User Agreement for Participation in an Electronic Communications System
(To Be Completed by Employees, Volunteers, and Students)

This user agreement must be renewed each academic year by employees, volunteers, and students.

Users Name:

Grade level:

School/Organization:

I have read the district's Acceptable Use Policy and Administrative Procedures and agree to abide by their provisions. I understand that violation of these provisions may result in disciplinary action including but not limited to suspension or revocation of privileges, suspension or expulsion from school, termination of employment, and criminal prosecution.

User's Signature:

_____

(To Be Completed by Parent/Guardian authorizing student access. This signature is required in addition to student signature above.)

Parent/Guardian Sponsor
I have read the district's Acceptable Use Policy and Administrative Procedures. In consideration for the privilege of using the district's system/network, emerging technologies, external networks sponsored by the district, and in consideration for having access to the public networks, I hereby release the district, its operators, and institutions with which they are affiliated from any and all claims and damages of any nature arising from my child's use of, or inability to use, the system/network, including, without limitation, the type of damage identified in the district's policy and administrative procedures.

_____ I give permission for my student to participate in the district's system/network.

_____ I do not give permission for my student to participate in the district's system/network.

Signature of Parent/Guardian:

First Reading	May 15, 1997
Second Reading:	Waived
Third Reading:	Waived
Policy Adopted:	May 15, 1997
Policy Amended:	April 5, 2007; July 17, 2008, January 6, 2011; June 2, 2011; January 24, 2013
Policy Reviewed	
Legal References:	MGL Chapter 4, Section 7(26); 950 C.M.R. 32
Policy Cross Reference:	JICFB (Bullying Prevention)
Procedure Reference:	

01/13/la