

HOPKINTON SCHOOL COMMITTEE POLICY

INTERNET ACCEPTABLE USE POLICY FOR STUDENTS & STAFF

The School Committee recognizes that Internet resources and various electronic tools including, but not limited to, laptop and tablet computers, “smart” phones, and digital cameras change how information may be created, accessed, communicated, and transferred. The School Committee supports the use of the district’s network and electronic tools by both students and staff for educational purposes and it recognizes that the District must assure that students develop the skills that are necessary to appropriately and safely analyze, evaluate, and utilize such resources. The School Committee expects that staff will blend thoughtful use of such information and tools throughout the curriculum and provide guidance and instruction to students in the appropriate use of both, including adherence to copyright and cyber-bullying laws.

The Hopkinton Public Schools shall not be liable for individual user’s inappropriate use of electronic resources or violations of copyright restrictions, users’ mistakes, or negligence or costs incurred by users.

As electronic tools and the Internet are constantly changing and the rate of change is increasing, this policy will be regularly reviewed to assure currency with new tools or Internet services.

Prohibited Behaviors

The School Committee charges the Superintendent or his/her designee with establishing, promoting, and adhering to regulations that maintain legal, ethical, and responsible use of the district’s electronic tools and network, and assuring that use conforms with Massachusetts and federal law and regulations, as well as the policies of the Hopkinton Public Schools. The district’s network or electronic tools may not be used for the following:

- **Harassment, discrimination, or bullying.** This includes, but is not limited to, the use of obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language or images that harass and discriminate against a protected class or constitute cyber-bullying.
- **Posting of personal information.** No student or staff member may use the network to post personal addresses, telephone numbers, or personal email addresses of oneself or others without express prior consent of the principal and parents.
- **Sharing of email accounts.** Staff and students will take reasonable precautions to maintain the security of email or other accounts provided by the district by keeping passwords confidential.
- **Plagiarism.** Text, graphics, video, or other content must be used in accordance with copyright law and properly cited.
- **Copying district-purchased and/or copyrighted software.**
- **Accessing confidential information.** No one may gain unauthorized access or intentionally seek information on, obtain copies of, or modify files, other data, or passwords for which the person has not been given access, or misrepresent other users on the network.
- **Illegal activity of any type.**

The following uses are generally prohibited, with limited exceptions:

- **Commercial or for-profit purposes, including advertising.** Students may not use the district network to offer, provide, or purchase products or services. However, a staff member may use the network for these purposes as their job requires.
- **Accessing inappropriate material.** Although the district network is filtered in accordance with the Children's Internet Protection Act, it may be possible to access material that is profane, obscene, or pornographic, that advocates illegal acts, or that advocates violence or discrimination towards other people. Such use is prohibited unless a teacher approves a specific, special exception for a student to conduct research.
- **Political lobbying for candidates.** The network may be used, however, within the rights of free speech to communicate with elected representatives and to express opinions on political issues.
- **Uploading or downloading unauthorized software on any district electronic device.** The Director of Technology may authorize downloading of software for district devices.

Social Networking

Staff will not:

- Fraternize with students using social networking sites such as, but not limited to, Facebook, MySpace, and similar Internet sites,
- Contact students via cell telephone, text, or instant message except in emergency or previously approved situations. Staff members who seek approval will complete a Social Network Contact Approval Form (IJNDB-R2), which must be signed by the Principal or Athletic Director.
- Make contact with students except through the district’s computer and telephone system, unless there is an emergency or if approved as described above.
- Give out private contact information without prior approval.
- Make inappropriate contact with staff, students, or parents including:
 - Sharing items with sexual content,
 - Bullying,
 - Harassing, or
 - Exhibiting or advocating use of drugs or alcohol.

Use of District Devices and Electronic Network

All data stored or transmitted on any district electronic device or transmitted from any device on the district network may be monitored, retrieved, downloaded, printed, copied at any time and without notice, as staff and students have no right to privacy with regard to such data. This information may be disclosed to others, including law enforcement agencies.

The use of the district’s network and electronic tools is a privilege, not a right. Access to network services will be provided to students and staff who demonstrate continual adherence to this policy. In addition, no student will be allowed to independently use the network unless parents or guardians provide Acceptable Network Use Permission (IJNDB – R1). Such permission may be provided on a paper copy or electronically in whatever format the district may provide.

First Reading	September 2, 2010
Second Reading	September 16, 2010
Third Reading	October 21, 2010
Adopted	Originally June 12, 2001; October 21, 2010
Policy Amended	
Legal References	Title 17 U.S. Copyright law Massachusetts General Laws:

	<p>c.66 §10 (public records)</p> <p>c.71 §37h1/2 (felony complaint or conviction of student)</p> <p>c.76 §5 (prohibiting educational discrimination in public schools)</p> <p>c.214 §1c (right to be free from sexual harassment)</p> <p>c.265§.43 (prohibiting stalking)</p> <p>c. 266:</p> <ul style="list-style-type: none"> ▪ §37e (use of personal identification of another) ▪ §98 (schoolhouse defacement) ▪ §120f (unauthorized access to computer system) ▪ §127 (personal property malicious or wanton injury) ▪ §143a (unauthorized reproduction or transfer of sound recordings) <p>c. 269 §17 (prohibiting hazing)</p> <p>c. 92 of the Acts of 2010, <i>An Act Relative to Bullying in Schools</i>; 603 CMR 49.00;</p>
Policy Cross Reference	<p>JICFB Bullying</p> <p>ACAB Harassment and Discrimination</p>
Procedure Reference	<p>Acceptable Network Use Permission Slip (IGNDB – R1)</p> <p>Social Network Contact Approval Form (IJNDB-R2)</p>