BELMONT PUBLIC SCHOOLS

**Office of Educational
Technology
(617) 993-5450**

221 CONCORD AVENUE
BELMONT MASSACHUSETTS 02478

**Steven Mazzola
Director of Technology
smazzola@belmont.k12.ma.us**

To: Belmont School Committee
From: Steven Mazzola, Director of Technology
Re: Update to Student Network Acceptable Use Policy
Date: January 18, 2011

Please find attached, an updated Student Network Acceptable Use Policy for your approval. The policy has been updated to better align it with the new district Anti-Bullying Policy, the Children's Internet Protection Act, and state regulation MA 201 CMR 17.

The changes occur in two places as detailed here:

1. On page 1, "Grades 5-12" is changed to: "Grades K-12".

2. On page 4, "This policy does not require a signature as it is referenced in the Belmont High School and Chenery Middle School student handbooks." is changed to: "This policy does not require a signature as it is referenced in each school's student handbook."

BELMONT PUBLIC SCHOOLS

Student Network Acceptable Use Policy
Grades K-12

I. Introduction

The Belmont Public Schools offers network access to its students, faculty, and staff. Access to the school network and the Internet is a privilege, not a right. The intent of this policy is to ensure that students utilize this access in a manner consistent with the purpose of providing this service. The Belmont Public Schools reserves the right to amend this policy.

II. Purpose

The primary purpose of the Belmont Public Schools Computer Network ("the Network") is to support the educational objectives of the Belmont Public Schools and Belmont's educational community in general. Network use provides valuable opportunities for research, curriculum support, and career development. The Network is not a public forum, and the Belmont Public School system reserves the right to place reasonable limits on materials posted or accessed through this network.

Additionally, this policy outlines the roles and responsibilities of students in a digital world through the norms of appropriate, responsible behavior with regard to technology use called Digital Citizenship. The themes of Digital Citizenship are: etiquette, communication, literacy, access, commerce, law, rights and responsibilities, health and wellness, and security[1].

To use the Network, students must take full responsibility for their own actions. While the network's possibilities are tremendous, it also has potential for abuse. The Belmont Public Schools shall not be liable for the actions of anyone accessing the network. Students assume full responsibility for any costs, liabilities, or damages arising from the way the student chooses to use their access to the Network.

A student's use of the Network constitutes their agreement to abide by this policy as set forth below, or as modified in the future.

---

[1] Ribble, Mike. "Nine Elements of Digital Citizenship." *Digital Citizenship; Using Technology Appropriately* 2010. Web. 5 April 2010

III. <u>Network Usage Guidelines</u>

Use of the Network must be consistent with its purpose as stated in Section II. This policy outlines acceptable use of the Network. However, it does not attempt to articulate all required or proscribed behaviors by students of the network. Students are expected to conform their actions with the purpose, spirit, and examples set forth in this policy and to abide by the rules of acceptable use, which include, but are not limited to, the following:

1. It is the policy of Belmont Public Schools to maintain a school environment free of harassment based on race, color, religion, national origin, age, gender, sexual orientation, disability, or any other characteristic protected by law. Students shall observe this policy in the use of the Network. Employ digital etiquette by using appropriate, non-abusive language, refrain from making defamatory remarks or racial slurs, bullying, and from the use obscene or profane language.

2. When using the Network, students shall identify themselves by their first names only. Do not reveal personal information such as last names, addresses, phone numbers, photos, etc. that could identify yourself, another student, or a staff member, except when required by a teacher to complete school-related work. You must immediately disclose to a teacher or other school staff, any message you receive that you believe is inappropriate or makes you feel uncomfortable.

3. Do not use the Network in such a way as to disrupt its use by others. Students must not vandalize school computers by causing physical damage, reconfiguring the computer system, or introducing malicious programs into the Network (for example, computer viruses).

4. Network IDs and passwords are provided for each user's personal use only. Passwords should not be shared with anyone. Students must not use another person's password. If you suspect that someone has discovered your password, you must have it changed immediately.

5. Any use for, or in support of, illegal purposes or activities is prohibited. This includes, but is not limited to, gaining unauthorized access to other systems, arranging for the sale or purchase of drugs or alcohol, participating in criminal gang activity, threatening others, transferring obscene material, or attempting to do any of the above.

6. Any use for commercial purposes is prohibited. Students may not create web pages to advertise or sell products or services and may not offer, provide, or purchase products or services through the Network.

7. Any use for political purposes is prohibited except for using the Network to communicate with elected officials.

8. Students should assume that most materials available on the Internet are protected by copyright. Unauthorized copying of copyrighted materials is prohibited. Additionally, any material obtained from the Internet and included in one's own work must be properly cited regardless of copyright status.

9. Not all material accessible through the Internet is of educational value. Students are expected to refrain from seeking, accessing, uploading, downloading, transmitting, or distributing material that is not relevant to their assignments or course work. No student may upload or download material to or from Internet sites without permission from their teacher.

10. Students shall not access, upload, download, transmit, or distribute material that is pornographic, obscene, sexually explicit, threatening, discriminatory, intimidating, abusive, harassing, or offensive.

11. Students must not access chat rooms or social networking sites. Students are also prohibited from using the Network to blog or to send or received instant messages. Games must not be played, accessed, or downloaded. The Belmont Public School System will take reasonable precautions to filter out inappropriate materials; however, it is impossible to monitor all content.

12. Students shall neither download nor install any commercial software, shareware or freeware onto network drives or disks without prior permission of the Director of Technology. Students shall not change settings on the browser or any other application.

13. Students shall not access, receive, upload, download, transmit, or distribute information pertaining to dangerous instruments such as bombs or other explosive devices, automatic weapons or other firearms, or other weaponry.

14. Students must not attempt to gain unauthorized access to any file servers or data in the Belmont Public Schools system, outside file servers or data, or go beyond the user's authorized access. This includes logging in through another person's account and/or accessing another person's files. Students shall not seek information on, obtain copies of, or modify files, other data, or passwords belonging to other students.

IV. <u>Privacy</u>

Students should not have an expectation of privacy or confidentiality in the content of electronic communications or other computer files sent and received and/or stored on the school computer network. Students should be aware that the data they create, receive, or send on the Network is the property of the Belmont Public School system, and that the data may be recovered and reviewed, even after it has been deleted. The Belmont Public School system also reserves the right to monitor use of the Network and to examine all data stored on district servers. All communications, regardless of content or purpose, are public and are not private. All communications including text and image may be disclosed to law enforcement or other third parties without prior consent of the sender or the receiver. Network administrators may review communications to maintain integrity system-wide and ensure that students are using the system in a responsible manner.

All network activities are logged. These logs may be disclosed to law enforcement or other third parties.

V. <u>Violations</u>

The system reserves the right to deny, revoke or suspend, without prior notification, specific user privileges and/or to take other disciplinary action, including suspension or expulsion from school, for violation of this policy. Additionally, all handbook regulations apply to use of the Network. In the event that there is a claim that a student has violated any of the guidelines in this policy, he or she will be provided an opportunity to be heard. The system will advise appropriate law enforcement agencies of illegal activities conducted through the Network. The Belmont Public School system also will cooperate fully with local, state, and/or federal officials in any investigation related to any illegal activities conducted through the Network.

VI. <u>Acceptance</u>

This policy does not require a signature as it is referenced in each school's student handbook.

Adopted by the Belmont School Committee, May 4, 2010