BELMONT PUBLIC SCHOOLS

Staff Technology Acceptable Use and Internet Safety Protocol

I. Introduction

The Belmont Public Schools offers network access to its users, faculty, and others such as volunteers and elected officials. Access to the school network and the Internet is a privilege, not a right. The intent of this protocol is to ensure that it is accessed in a manner consistent with the purpose of providing this service. The Belmont Public Schools reserves the right to amend this protocol and is to be used in conjunction with the School Committee Technology Use and Internet Safety protocol.

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 (although its contents may be disclosed as a public record), and the Belmont Public School system reserves the right to place reasonable limits on materials posted or accessed through this network. The Belmont Public School System will take reasonable precautions to filter out inappropriate materials; however, it is impossible to monitor all content.

This protocol outlines the roles and responsibilities of users 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].

When accessing the network, users 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. Users assume full responsibility for any costs, liabilities, or damages arising from the way the user chooses to access to the network. Use of the network constitutes their agreement to abide by this protocol 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. Safeguarding Student Information and Student Access

Furthermore, this protocol seeks to educate staff about online content monitoring and ensuring student personal information is not disclosed; as required under the Children's Internet Protection Act and the Family Educational Rights and Privacy Act. Staff are expected to monitor student internet use in such a manner to prevent access by minors to inappropriate matter on the internet, including attempts to access inappropriate materials and circumvent system security; and provide instruction to students on interacting with other individuals on social networking websites and in chat rooms, and response to cyberbullying.

IV. Network Usage Guidelines

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

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

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

3. 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, information about dangerous materials or devices such as weapons, threatening others, transferring obscene material, or attempting to do any of the above.

4. Any use for commercial purposes is prohibited. Users 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.

5. Any use for fundraising for any non-school sponsored purpose, whether for charity or otherwise is prohibited.

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

7. Downloading, using, or copying software in violation of a license agreement or copyright, or otherwise infringing on intellectual property rights is prohibited.

8. Users 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. Users are expected to refrain from seeking, accessing, uploading, downloading, transmitting, or distributing material that is not relevant to their work.

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

11. Staff must obtain the permission of their supervisor or supervisor's designee prior to creating, publishing, or using any district web pages, social media pages or any other digital content which is school-related, or which could be reasonably understood to be school-related. This includes any content which identifies the school or affiliated club, team, or organization by name in the account name or which uses the school's name or image. When creating accounts, staff must use an official Belmont Schools e-mail address and confirm the proper use of privacy settings with the approving supervisor or supervisor's designee. No social media account covered by this protocol shall permit comments by the public unless otherwise approved by a supervisor or supervisor's designee.

    Staff may be required to provide their supervisor or supervisor's designee with the username and password to district social media accounts. However, staff may not provide the username and password to district accounts to any unauthorized individual, including students and volunteers.

    Any student-related content, including pictures, is subject to the same restrictions governing the Web Page Protocol and a parent's decision to opt their student out of certain publications. Each school office maintains a list of students whose parents have

opted-out of publication. It is the staff member's responsibility to check that list before posting such information.

Social media accounts should be used exclusively for the district and classroom-related work and communication. Staff members may not use district accounts for personal use.

Staff shall not access social media networking sites on school-owned devices unless such access is for an educational activity which has been pre-approved by a supervisor or supervisor's designee. This prohibition extends to using chat rooms, message boards, messaging in social media applications, and includes posting on social networking sites.

Users shall be aware of their use of social media; as others may conduct their own search of you. Such searches may result in discovery of personal postings and/or your comments made about work, fellow staff/users, and/or students. Given such possible searches and your status as a school district employee, staff are held to a higher standard of conduct that reflects on your reputation and/or that of the school district. Users shall refrain from "friending" or creating other electronic relationships with students; including the use of personally-identifiable information such as home addresses and telephone numbers.

12. Users shall neither download nor install any commercial software, shareware or freeware onto network drives or disks without prior permission of the Director of Technology. Appropriate educational apps may be downloaded to your iPad without prior permission.

13. Staff shall not connect any device not owned and managed by the school district to the network (apart from use of wi-fi wireless network).

14. Users 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.

15. Users 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. Users shall not seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users.

16. Users are to access the district network only for purposes related to the schools and the performance of their jobs. Incidental personal use of school information technology is

permitted as long as such use is not excessive, wasteful, and/or otherwise does not interfere with the employee's job duties and performance and is in accordance with the policies set forth in this protocol. Incidental personal use is defined as use by an individual employee for occasional personal communications (see personal use restrictions in section 9). Personal means of communication should not be used to conduct district-related business.

17. Use appropriate judgment and caution in communications concerning students and ensure that personally identifiable information remains confidential. In order to limit the possibility of the disclosure of student records, student information shall be transmitted and stored only on systems and devices approved by the district. Student information should not be stored in an unsecured manner such as CDs, DVDs, USB drives, other portable media, or on personal devices.

V. Privacy

Users should not have an expectation of privacy or confidentiality in the content of electronic communications or other computer files sent or received and/or stored on the school computer network. Users 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 captures and archives all e-mail, including attachments, sent and received through the district's mail servers and also reserves the right to monitor use of the network and to examine all data stored on district servers or other systems maintained by third parties under contract with the district.

Any e-mails or other communication or data may be a public record and thus possibly subject to public disclosure. All communications, including text and images, regardless of content or purpose, are public, not private and may be disclosed to law enforcement or other third parties without prior consent of the sender or the receiver. Network administrators or their designees may review communications to maintain integrity system-wide and to ensure users are accessing the system in a responsible manner. All network activities are logged. These logs may be disclosed to law enforcement or other third parties.

VI. Violations

The district reserves the right to deny, revoke or suspend, without prior notification, specific user privileges and/or to take other disciplinary action, up to and including suspension or dismissal, for violation of this protocol. 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. Any known breach of this protocol should be immediately reported to the Director of Technology.

VII. Acceptance

Signature should be entered on the electronic Staff Update form issued to all staff annually.

Original protocol adopted by the Belmont School Committee December 8, 1998.
Revised September 7, 1999.
Updated protocol reviewed by the Belmont School Committee June 10, 2014.
Updated protocol reviewed by the Belmont School Committee September 11, 2018.