BARNSTABLE PUBLIC SCHOOLS
STAFF COMPUTER/NETWORK
ACCEPTABLE USE POLICY

The Barnstable Public Schools (District) has provided its staff with access to computers, email, an internal network, and the Internet. This District Network (the Network) has been provided to enhance the educational experience of our students. The Network is intended to assist teachers and students to meet the learning objectives of the district. With this in mind, any use of the Network that intentionally disrupts or interferes with the educational process is prohibited. The Child Internet Protection Act (CIPA) requires the development of a policy to provide guidelines for use of the Network.

Internet and Email

Network users have no expectation of privacy in any materials (email, attachments, documents, websites etc) that are stored, transmitted, or received via the District's Network or computers or personally-owed computers used by staff on District premises. The District reserves the right to monitor, inspect, copy, review, and store, at any time and without prior notice, any and all usage of District computers, systems, networks, and Internet access or personally owned computers used on District premises and any and all information transmitted or received in connection with such usage. This shall include communications made through a user's personal web-based email account (such as Hotmail or Yahoo! Mail) specifically via the District's network or computers and communications made to or from a user's personal home-based computer specifically over the District's network.

The District is required to, has the capability, and reserves the right to monitor use of the Internet, including web sites visited and files downloaded via the District's network. Users should understand that the deletion of a message or file may not eliminate it from the system. The network may not be used to violate any law, regulation, or District policy. The District is mandated by federal law to filter all Internet access within it's system. This is done to protect students from access to sexually explicit, offensive or otherwise inappropriate Web sites. Network users are not permitted to visit such sites. In addition the District attempts to block all social networking sites such as My Space.com because of the dangers they pose to children's safety. Users who find that such a site is not filtered should contact the District's Department of Educational Technology so it can be blocked. Likewise if an educationally appropriate site has been filtered or blocked, users may contact the department so the site can be unblocked if approved.

The Network may not be used to send, display or receive offensive messages, pictures or other media which are defamatory, abusive, obscene, profane, sexually orientated, threatening, racially offensive or intended to harass or intimidate. The Network may not be used to transmit material in violation of federal or Massachusetts law or regulation,

such as the transmission and dissemination of copyrighted material. This policy also includes web pages, blogs, wikkis, Podcasts, etc.

Faculty and staff shall be familiar with the Student Acceptable Use Policy which will be provided to staff by the District. Teachers shall monitor their students when using computers during their classes, to prevent downloading games, viruses, spyware and theft and vandalism to the hardware. All staff shall assist with the supervision of students who are assigned to them on computers and report any Student AUP violations immediately to the Principal, House Master or Prevention Specialist as appropriate to the building.

Hardware

Staff members will be diligent within their schedules in protecting any and all hardware issued by the District (including but not limited to computers, handhelds, cameras, printers, projectors and scanners) and safeguard such from theft, loss or damage. Staff should not download material or install software without permission from the District Educational Technology Department. All software on the District computers is to be used for educational purposes and support the educational goals of the District. Downloaded material (including but not limited to mp3, weather bug, games, and .wav files) can infect individual computers and the Network. It is the responsibility of network users to help protect the Network from such viruses, spyware, adware, etc. to the extent possible. Employees shall follow software licensing agreements of which the employer has made them aware and where necessary has provided training.

Staff who wish to purchase or bring in their own equipment (for example: computers, external drives, printers, wireless) must consult with and get approval from the District Educational Technology Department; this is to insure that the hardware is compatible with and will not harm the Network. Likewise staff are not allowed to install personally owned software without the approval of the District Educational Technology Department in writing. The installation of such software may be in violation of licensing agreements or may hinder computer performance or Network access. The Educational Technology department will support and maintain equipment that is purchased with the consent of the Department.

It is the responsibility of the staff to maintain backup copies of their files. This means they can save to the “P drive” or save files to a memory card, CD etc. Individual staff members are also responsible for the reinstallation of software that they have purchased with the approval of the Educational Technology Department in writing. This is because the computer may be “swapped out” or replaced at the discretion of the Educational Technology Department for repair, maintenance or redistribution.

General examples of proper network behavior are:

- Be polite.
- Use appropriate, non abusive language.

- Be cautious about revealing personal addresses, credit card numbers, or phone numbers.
- Send information that other users will not find offensive.
- Obey copyright laws, fair use policies and follow licensing agreements.
- Do not tamper with the system, alter, “hack”, delete or destroy any files or data that are not yours.
- Do not knowingly introduce electronic worms and/or viruses to the system.
- Be considerate of our network resources and limit their demands on “bandwidth” and server space.

Network users should be aware that:

- Use of the network and e-mail is a privilege.
- The BPS network is to be used only for educational purposes
- E-mail is not guaranteed to be private. There is no expectation of privacy on the network.
- Identifying photos of students with their first and last names may not be used on a web site.
- Persons issued an account are responsible for its use at all times. Therefore it is important to log off the computer at the end of every session, so another user can not use your password.
- Staff computers that have programs that can access student records on such as Admin Plus and GradeQuick should not be used by students and should be logged off when unattended.

The District makes no warranties of any kind, whether expressed or implied, for the service it is providing. The District will not be responsible for any damages a user may suffer, including loss of data. The District will not be responsible for the accuracy or quality of information obtained through the internet connection.

Consequences

This policy has been developed to promote the legal and ethical use of a powerful education tool. It is not meant to limit the use of the global informational community but to ensure a safe environment for the children in our care. A violation of this policy may result in disciplinary action ranging from a verbal warning or suspension of system privileges up to discharge from employment in accordance with applicable legal and contractual procedures. When applicable, law enforcement agencies may be involved. Use of the District’s network by any staff or user shall constitute acceptance of the terms of this policy.

Signature: _____

Print name: _____

Date: _____