

The District technology system consists of software, hardware, computer networks and electronic communications systems. Use of the District technology system is a privilege, not a right. All use of this system, including independent use off school premises, shall be subject to this policy and accompanying regulations. Student and staff use is for **school-related purposes only**, supporting our **students' educational program and staff's professional development**. Failure to comply with District Policy and Administrative Regulations for use of the District's technology system will result in corrective action, ranging from verbal reprimand up to and including loss of school privileges including computer privileges, detention, suspension from school, and, where warranted, other civil and/or criminal proceedings.

The Superintendent, the Instructional Technology Coordinator or their designees shall monitor and examine all network activities as deemed appropriate to ensure proper use. They shall disseminate and, in conversation with the District Technology Committee, interpret district policy and regulations governing the use of the district's network at the building level with all network users. They will appoint teachers, other staff members and students to help monitor and troubleshoot technology related problems. They will ensure that a staff development program encompassing all aspects of the District technology resources is in place throughout the school year. They shall make certain that proper network tools are in place to protect against access to inappropriate Internet sites and to safeguard the District network from malicious outside attack and virus infections.

All users shall adhere to the laws, policies and rules governing computers including, but not limited to, copyright laws, rights of software publishers, license agreements, and rights of privacy created by federal and state law.

All users' data files stored and maintained by the District shall be considered to be District property and will be subject to District control and inspection. The Instructional Technology Coordinator may access all such files and communications to insure system integrity and that users are complying with the requirements of this regulation. Users should NOT expect that information stored on the District technology system will be private.

Security on the District technology system is a high priority, especially when the system involves many users. Users identifying a security problem on the District's system must notify the teacher in charge or a network technician. A user is not to demonstrate the problem to other users. Attempts to log on the District's technology system as a network administrator will result in cancellation of user privileges. Any user identified as a security risk or having a history of problems may be denied access to the District's technology system.

All users must agree to abide by district policy and regulations.

STAFF USE OF DISTRICT TECHNOLOGY SYSTEM

Generally, the same standards of acceptable staff conduct which apply to any aspect of job performance shall apply to use of the District's technology system. Employees are expected to communicate in a professional manner consistent with applicable District policies and regulations governing the behavior of school staff. Electronic mail and telecommunications are not to be utilized to share confidential information about students or other employees.

STUDENT USE OF DISTRICT TECHNOLOGY SYSTEM

One purpose of these regulations is to provide notice to students and parents/legal guardians that, unlike most traditional instructional or library media materials, the District technology system will allow student access to external computer networks not controlled by the School District where it is impossible for the District to screen or review all of the available materials. Some of the available materials may be deemed unsuitable by parents/legal guardians for student use or access. These regulations are intended to establish general guidelines for acceptable student use. It will not be possible to completely prevent access to computerized information that is inappropriate for students. Furthermore, students may have the ability to access such information from their home or other locations off school premises. Parents/ legal guardians of students must be willing to set and convey standards for appropriate and acceptable use to their children when using the District's technology system or any other electronic media or communications.

Students who engage in unacceptable use may lose access to the District's technology system and may be subject to further discipline under the district's school conduct and discipline policy. The District reserves the right to pursue legal action against a student who willfully, maliciously or unlawfully damages or destroys District property.

SUBJECT: STUDENT AND STAFF USE OF DISTRICT TECHNOLOGY SYSTEM - PROHIBITIONS

1. Using the District's technology system to obtain, view, download, send, print, display or otherwise gain access to or to transmit materials that are unlawful, obscene, pornographic or abusive.
2. Use of obscene or vulgar language across the network via e-mail or other sources.
3. Harassing, insulting or attacking others across the network via e-mail or other sources.
4. Damaging, disabling or otherwise interfering with the operation of computers, computer systems, software or related equipment through physical action or by electronic means.
5. Using unauthorized software on the District's technology system.
6. Changing, copying, renaming, deleting, reading or otherwise accessing files or software not created by the student without express permission from the computer coordinator.

7. Violating software and copyright law.
8. Employing the District's technology system for commercial purposes, product advertisement or political lobbying.
9. Disclosing an individual password to others or using others' passwords. Network accounts are to be used only by the authorized owner of the account.
10. Transmitting material, information or software in violation of any District policy or regulation, the school behavior code, and/or federal, state and local law or regulation.
11. Revealing personal information about oneself or of other students including, but not limited to, disclosure of home address and/ or telephone number.
12. System users shall be allocated resource disk space quotas as set by the administration. Such quotas may be exceeded only by requesting to the appropriate administrator or system coordinator that disk quotas be increased and stating the need for the increase.

Personal Equipment

The District will allow personal notebook computers, **from staff members only**, after a review by a district technician. We will review their virus software and if deemed not adequate we will ask them to update or we will install a licensed copy of our district software. We make it clear that if after being configured to our school network if they then have problems with their home network or internet connection that they would need to contact their provider and have their home connection corrected. If after being corrected they now have trouble with the school connection, we recommend that we do not try and reconfigure again to our network. They can then use it in the classroom but we will not support it or allow it to be connected to our network. Everyone must again have their equipment reviewed at the beginning of the next school year.

Any desktop computer that is brought in for classroom use will be reviewed to see if it meets our minimum standards. If it meets that requirement, it will be considered donated to the district and configured to the network (including system software). If it does not meet minimum standards or they are not interested in donating it to the district, they can use it in the classroom but again, we will not support it or allow it to be connected to our network.

Users are **NOT** allowed to use flash drives, floppy disks or any other storage device on the District's network without first confirming that they are virus free. When necessary, students will seek advice from the technology department as to the best way to access and print their files from home and otherwise access network resources. Instruction will be available for the transfer of files between home and school.

Web Guidelines

BH-BL websites provides a communication link with all elements of our school community. Our websites provide links with alumni, parents, school staff, students, community members

and audiences around the world. Therefore, it is essential to establish guidelines to ensure a high quality of communication and to protect the rights of our community.

Guidelines serve multiple purposes:

- to ensure the accuracy of information.
- to maintain current information.
- to promote and support the BH-BL mission statement.
- to protect the privacy of students.
- to ensure the safety of students.

All web content must conform to all existing BH-BL policies and any appropriate local, state or federal laws. These policies and laws include but are not limited to copyright, civil rights and privacy issues.

Guidelines for Content

All material on web pages must pertain to curriculum, school related activities, school announcements and any other materials related to the mission and environment of Burnt Hills-Ballston Lake Central School District. Faculty or student work may be published only as it relates to curriculum or school related projects. Therefore, neither staff nor students may publish personal home pages identified in any way as being part of the BH-BL web site. Home pages for other individuals or organizations not directly affiliated with the district shall also not represent themselves as being district sponsored.

Since the website will be a visual symbol of District programs, activities and beliefs, please adhere to the following guidelines:

- All staff home pages must be posted through First Class or exist on a district or BOCES server. Teachers who currently have personal web pages on private internet providers should contact the District's Technology Coordinator to transfer appropriate files to a district server.
- Student web pages must be supervised and approved by a teacher as part of a school assignment. The page can only reside on a district or BOCES server.
- All Web page work must be well written and be free of spelling and grammatical errors. Documents may not contain objectionable material or link to objectionable material. Decisions concerning objectionable materials will be decided by the principal or her/his designee.
- Corrections and updates must be made in a timely fashion.
- Any materials owned by others or copyrighted works may not be used without express written permission of the owner.
- Commercial activity is not permitted on any pages unless related to course requirements. The site is intended for BH-BL purposes and not for the benefit of individuals or other organizations.

- The BH-BL name must not be used in any way to suggest or imply endorsement of other organizations, products or services.
- Fundraising announcements that may appear as part of the district web pages are limited to those for PTAs and official school organizations. All such announcements must be specifically approved in writing by the building principal or superintendent.
- Huge, bandwidth-clogging photos or graphics should be avoided.

The District requests that all sites containing school related activities or information conform to the above guidelines. This would include booster clubs, community and other independent organizations.

Guidelines for Publishing

Student photographs may appear on the BH-BL Web Site only if written permission is first obtained from parents. It will be the responsibility of the page author to:

1. Obtain the written permission (using BH-BL's standard permission for student photography form that is available on the website); **and**
2. Keep the signed form on file for at least the time between the consent and the student's eighteenth birthday in the permanent record file.

At the elementary level, teachers are required to send permission forms home at the start of the school year so they will know who can, and cannot, be photographed in their classrooms. Elementary permission forms need to be renewed on an annual basis. At the secondary level, teachers are required to get signed permission form on an as-needed basis.

- Identification of students on web pages will be limited to a student's first name and first initial of his/her last name. The only exceptions are for on-line versions of print publications such as school and district newsletters. In special situations, other exceptions may be made, but only with parental permission.
- Web pages may not include students' ages, telephone numbers, addresses, names of other family members or last names of friends.
- Published e-mail addresses are restricted to staff members. Only First Class e-mail addresses should be published. Web pages may not contain any student e-mail addresses or other direct-response links back to students.

Guidelines for Student/Faculty Use

General Guidelines

- Students may participate in only those Internet exchanges approved by school personnel.
- Any Internet security problems must be reported to a teacher, lab aide or principal.
- E-mail exists on the BH-BL server for educational purposes.

- Electronic transmission of materials is a form of copying. As specified in district policy, no unlawful copies of copyrighted materials may be knowingly produced or transmitted via the district's equipment, including its web server.
- All communications via the BH-BL web site will comply with Board of Education policy P5311, Student Responsibility and Freedom of Expression. Offensive material that is expressly prohibited by this policy includes religious, social or sexual material, as well as any incitement to violent or illegal acts.

Prohibited Activities

Students are not allowed to promote activities against district policies or local, state or federal laws. Prohibited use of the computers and computer services shall include, but not be limited to:

- Subscriptions to listservs using school accounts without authorization
- Hosting of usenet groups and listservs without authorization
- Unauthorized use of e-mail
- Unauthorized use of web sites or web pages
- Unauthorized access to non-curricular related materials or resources
- Plagiarism or infringement of copying laws
- Use of chat rooms unless approved by building principal
- Other activities as determined by the District and amended to these guidelines.

Approved August 24, 1999

Renumbered from AR5590 and reviewed May 2000

Revised October 2006