RESPONSIBLE USE OF TECHNOLOGY AR4526

The Burnt Hills – Ballston Lake Central School District will use electronic resources as powerful and compelling tools for students to further understand all subjects and apply skills in relevant and rigorous ways. It is the District's goal to provide students with rich and ample opportunities to use technology as individuals do in workplaces and other real-life settings. The District's technology will enable educators and students to communicate, learn, share, collaborate and create, think and solve problems, manage their work, and take ownership of their lives.

These regulations are written to promote positive and effective digital citizenship among students and staff. Digital citizenship represents more than technology literacy: successful, technologically fluent digital citizens live safely and civilly in an increasingly digital world. They recognize that information posted on the Internet is public and permanent and can have a long-term impact on an individual's life and career. Expectations for student and staff behavior online are no different from face-to-face interactions. Access to the school's technology resources is a privilege. All activities conducted using BH-BL resources are subject to monitoring by the District.

This Administrative Regulation is not intended to interrupt or inhibit classroom teaching and learning. If you feel that any of the stated policy prohibitions affect your ability to deliver prepared classroom lessons, please contact your Dept./Bldg. Supervisor or the District Instructional Technology Coordinator to ensure that a working solution can be implemented.

If a staff member or student is unsure whether a contemplated activity may be in violation of stated policies, he/she should contact his/her teacher, Dept./Bldg. Supervisor and/or the District Instructional Technology Coordinator to ensure that this activity can be implemented.

Technology Resources

District technology resources include (but are not limited to) the transmission infrastructure, wired and wireless equipment, files and storage, e-mail and Internet content (blogs, web sites, web mail, groups, wikis, etc.). The District reserves the right to prioritize the use of, and access to, all technology resources.

All use of district technology resources must support academic or classroom activities, educational research and other learning opportunities consistent with the educational mission of the District.

All staff and student personal devices must be authenticated on the District's network. Personal devices must be equipped with up-to-date virus software, compatible network card and configured properly. Non-compliant devices will be removed. Connection of any personal electronic device is subject to all guidelines in this document. Expectations for responsible use remain the same, whether a personal or district device is used. The District will not be responsible for personal property that is lost, stolen or damaged. The District will not be responsible for unauthorized financial obligations resulting from District-provided Internet access.

Acceptable uses of technology resources by District students and staff include:

- Creation of files, projects, videos, web pages and podcasts using network resources in support of educational research.
- Participation by staff in blogs, wikis, bulletin boards, social networking sites and groups and the creation of content for podcasts, e-mail and web pages that support the mission of the district.
- Participation by students in **District-approved** blogs, wikis, bulletin boards, social networking sites and groups and the creation of content for podcasts, and web pages that support the mission of the district.
- Publication online of original educational material, curriculum-related materials and student work. Sources outside the classroom or school must be cited appropriately;
- Use of technology resources by staff for incidental personal use in accordance with all district policies and guidelines.

Unacceptable uses of technology resources by district students and staff include but are not limited to:

- Cyberbullying or cyberthreatening
    - Material, either in the form of text or images, posted on personal web sites, social networking sites, blogs or transmitted via email, discussion groups, message boards, chat rooms, instant messages, or via cellular phones in prohibited.
    - The use of the District's Internet system, cellular devices on school district property, cellular devices not on district property or the use of an Internet system not owned or operated by District to bully or harass other students, faculty and staff is prohibited.
    - Off-campus cyberbullying or cyberthreats - regardless of the form in which the message is transmitted - endangering the health, welfare or safety of students, faculty or staff within the District or adversely affecting the educational process is prohibited. Students engaging in this type of conduct will be disciplined according to the District's Code of Conduct or as outlined within this policy.
- Using network resources for personal gain, commercial solicitation and compensation of any kind;
- Downloading, installation and use of inappropriate games, audio files, video files or other applications (including shareware or freeware) without permission or approval from administration;
- Supporting or opposing ballot measures, candidates and any other political activity;

- Hacking; cracking; vandalizing; introducing viruses, worms, Trojan horses, time bombs; and changing hardware, software, and monitoring tools;
- Attempting unauthorized access to other district computers, networks and information systems;
- Posting, sending or storing information online that could endanger others (e.g., bomb construction guides, drug manufacture guides);
- Changing, copying, renaming, deleting, or otherwise accessing others' files.
- Accessing, uploading, downloading, storing and/or distributing of obscene or pornographic material; and
- Attaching unauthorized equipment to the district network.

The District will not be responsible for any damages suffered by any user, including but not limited to, loss of data resulting from delays, non-deliveries, mis-deliveries or service interruptions caused by its own negligence or any other errors or omissions.

Internet Safety: Personal Information and Inappropriate Content

Contributions to the Internet leave a digital footprint for all to see, therefore:

- Students and staff should not reveal personal information including a home address and phone number on web sites, blogs, podcasts, videos, wikis, e-mail or as content on any other electronic medium.
- Students and staff should not reveal personal information about another individual on any electronic medium.
- No student pictures or names can be published on any class, school or district web site unless the appropriate permission has been verified according to District policy.
- Students who encounter dangerous or inappropriate information or messages should notify the appropriate school authority.

Filtering and Monitoring

Filtering software is used to block or filter access to visual depictions that are obscene and all child pornography in accordance with the Children's Internet Protection Act (CIPA). Other objectionable material could be filtered. The determination of what constitutes "other objectionable" material is a local decision.

- Filtering software is not 100% effective. While filters make it more difficult for objectionable material to be received or accessed, filters are not a solution in themselves. Every user must take responsibility for his or her use of the network and Internet and avoid objectionable sites;
- Any attempts to defeat or bypass the District's Internet filter or conceal Internet activity are prohibited. This includes but is not limited to: proxies, https, special ports, modifications to district browser settings and any other techniques designed to evade filtering or enable the publication of inappropriate content;

- E-mail inconsistent with the educational and research mission of the District will be considered SPAM and blocked from entering District e-mail boxes;
- The District will provide appropriate adult supervision of Internet use. The first line of defense in controlling access by minors to inappropriate material on the Internet is deliberate and consistent monitoring of student access to district computers;
- Staff members who supervise students, control electronic equipment or have occasion to observe student use of said equipment online, must make a reasonable effort to monitor the use of this equipment to ensure that student use conforms to the mission and goals of the District; and
- Staff must make a reasonable effort to become familiar with the Internet and to monitor, instruct and assist students effectively.

Copyright

Downloading, copying, duplicating and distributing software, music, sound files, movies, images or other copyrighted materials without the specific written permission of the copyright owner is generally prohibited. However the duplication and distribution of materials for educational purposes are permitted when such duplication and distribution fall within the Fair Use Doctrine of the United States Copyright Law (Title 17, USC) and content is cited appropriately.

All student work is copyrighted. Permission to publish any student work requires permission from the parent or guardian.

Network Security and Privacy

Passwords are the first level of security for a user account. System logins and accounts are to be used only by the authorized owner of the account, for authorized district purposes. Students and staff are responsible for all activity on their account and must not share their account password.

These procedures are designed to safeguard network user accounts:

- Change passwords according to district policy;
- Do not use another user’s account;
- Do not insert passwords into e-mail or other communications;
- Be sure to keep passwords out of sight if you write them down;
- Do not store passwords in a file without encryption;
- Do not use the “remember password” feature of Internet browsers; and
- Lock the screen, or log off if leaving the computer.

Student Data is Confidential

District staff must maintain the confidentiality of student data in accordance with the Family Education Rights and Privacy Act (FERPA).

No Expectation of Privacy

The District provides the network system, e-mail and Internet access as a tool for education and research in support of the District's mission. The District reserves the right to monitor, inspect, copy, review and store, without prior notice, information about the content and usage of:

- The network;
- User files and disk space utilization;
- User applications and bandwidth utilization;
- User document files, folders and electronic communications;
- E-mail;
- Internet access; and
- Any and all information transmitted or received in connection with network and e-mail use.

No student or staff user should have any expectation of privacy when using the District's network. The District reserves the right to disclose any electronic message to law enforcement officials or third parties as appropriate. All documents are subject to the public records disclosure laws of the State of New York.

Archive and Backup

Backup is made of all district e-mail correspondence for purposes of public disclosure and disaster recovery. Barring power outage or intermittent technical issues, staff and student files are backed up on district servers nightly – Monday through Friday. Refer to the District retention policy for specific records retention requirements.

Disciplinary Action

All users of the District's electronic resources are required to comply with the District's policy and regulations and agree to abide by the provisions set forth in the District's Responsible Use Agreement.

Violation of any of the conditions of use explained in the District's Responsible Use Agreement or in these procedures could be cause for disciplinary action, including arrest, suspension or expulsion from school and suspension or revocation of network and computer access privileges.

Revised June 2011
Revised & Renumbered from AR5390 – September 2016