Acceptable Use of Electronic Information and Access

The Ballston Spa Central School District is committed to meeting the educational needs of each student in becoming a responsible adult. In partnership with the family and community, we strive to prepare each student intellectually, emotionally, physically and socially, while encouraging individual talents and abilities. In keeping with the mission statement, the district considers computer networks and the Internet to be a valuable tool for education and encourages the use of computer technology. Students have the privilege of working with the computer network and Internet in individual classrooms, libraries and labs to help perform academic work, to explore educational topics and to conduct research projects. With access to computers and people from around the world, also comes the availability of material that may not be considered to be of educational value. As required by the Children's Internet Protection Act (http://www.fcc.gov/cgb/consumerfacts/cipa.html), the Ballston Spa School District will use Internet filters to block or filter Internet, or other forms of electronic communications at school to help ensure a safer environment. The district is not responsible for inappropriate content accessed on personal electronic devices via an unfiltered Internet or cellular connection.

The smooth operation of computer resources relies upon the proper conduct of students. These guidelines are provided here so that you are aware of the responsibilities. The privilege of using computer technology in school may be limited at any time if a student fails to comply with district policy and regulations.

To gain access to the Ballston Spa computer network and Internet, students each year must read and follow the guidelines. Students will sign the attached document (Appendix 1/2) along with their respective parent or guardian each year. This document will be provided and kept on file in their respective school building.

In accordance with the Ballston Spa Central School District policy on Responsible Use of Electronic Information and Access (File 6.4.4) and Code of Conduct (File 7.10) the following guidelines are established:

A. Personal Safety

  1. Users will not post personal contact information about themselves or other people. Personal contact information includes personal address, personal telephone number, etc.

  2. Users will not arrange to meet with a stranger they have met online.

  3. Users will promptly disclose to their teacher or other school employee any message they receive that is inappropriate or makes them feel uncomfortable.

B. Illegal Activities

   1. Users will not attempt to gain unauthorized access to the district system or to any other computer system through the district system, or go beyond their authorized access. This includes attempting to log in through another person's account or access another person's files. (These actions are illegal, even if only for the purposes of "browsing.")

   2. Users will not make deliberate attempts to disrupt the computer system performance or destroy data by spreading computer viruses or by any other means. (These actions are illegal.)

   3. Users will not use the district system to engage in any other illegal act, such as arranging for a drug sale or the purchase of alcohol, engaging in criminal gang activity, threatening the safety of person, etc.

   4. The illegal installation of copyrighted software or files for use on district computers is prohibited.

C. System Security

   1. Users are responsible for the use of their individual account and should take all reasonable precautions to prevent others from being able to access their account. Under no conditions should a user provide their password to another person unless that person is an authorized technology system administrator.

   2. Users will immediately notify the supervising adult or the district technology office if they have noted a possible security problem. Users should not demonstrate or discuss the problem to anyone besides the supervising adult or the district Technology Office.

   3. Users will not download or install software or other files unless directed to do so by the District Technology Office.

   4. No personal devices will be connected to the district network without the authorization of the district Technology Office. Users with authorization to connect personal devices to the district network are subject to the guidelines outlined in this document.

   5. No district owned computing device will be used off the district network without proper permission and/or signed paperwork.

D. Inappropriate Language
   1. Users will not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language.

2. Restrictions against inappropriate language apply to public messages, private messages, and material posted on web pages.

3. Users will not post information that, if acted upon, could cause damage or disruption.

4. The Dignity for All Students Act (2010) prohibits activities that create a hostile environment at school and school sponsored events. Users will not engage in personal attacks, including prejudicial or discriminatory attacks.

5. Users will not harass another person. Harassment is persistently acting in a manner that distresses or annoys another person. If a user is told by a person to stop sending those messages, they must stop.

6. Users will not knowingly or recklessly post false or defamatory information about a person or organization.

7. The use of mobile device cameras (personal or district owned) on district property to take or store a picture of anyone, with-out first obtaining that persons explicit permission is strictly prohibited.

E. Respecting Resource Limits

1. Users will use the system only for educational and professional or career development activities, and limited, high-quality, self-discovery activities. Assigned educational activities will take priority over self-discovery activities.

2. Users will download large files only under the supervision of a teacher and only when absolutely necessary. If necessary, users will download approved files at a time when the system is not being heavily used and immediately remove the file from the network computer to their personal storage device.

3. Users will not post chain letters or engage in "spamming." Spamming is sending an annoying or unnecessary message to a large number of people.

4. Student use of email, chat, messaging, and web-authoring will be limited to pre-approved curriculum-related projects that are supervised by a teacher.

5. Users will subscribe only to high quality discussion group mail lists that are relevant to their education or professional/career development.

F. Plagiarism and Copyright Infringement

1. Users will not plagiarize works of others. Plagiarism is taking the ideas or written material of others and presenting them as if they were original to the user.

2. Users will respect the rights of copyright owners. Copyright infringement occurs when an individual inappropriately reproduces a work that is protected by a copyright. If a work contains language that specifies acceptable use of that work, the user should follow the expressed requirements. If the user is unsure whether or not they can use a work, they should request permission from the copyright owner.

G. Inappropriate Access to Material

1. Users will not use the district system to access material that is profane or obscene (pornography), that advocates illegal acts, or that advocates violence or discrimination towards other people (hate literature).

2. If a user inadvertently accesses such information, they should immediately disclose the inadvertent access to the supervising adult or the District Technology Office.

3. The district will use filtering software as required by the Children's Internet Protection Act. The district reserves the right to limit or deny access to any site that it deems inappropriate or outside the scope of the district's mission to educate children.

4. The use of cellular data or any non-district Internet provider is prohibited on school grounds.

5. Users will not attempt to use Proxy sites to bypass district firewalls.

H. Due Process

1. Violations of this policy may result in restrictions on access to the district's electronic resources.

2. Disciplinary action will be implemented in line with district policy (Section 7.10-Code of Conduct) and procedures established at the building level.

3. When applicable, law enforcement agencies may be involved.

4. Damage caused by inappropriate or careless use will be the fiscal responsibility of the user.

I. Privacy and Confidentiality

The district reserves the right to inspect and examine any school owned or operated communications system computing resource and/or files or information contained therein at any time. When sources outside the district request such information, the district will treat information as confidential unless one or more of the following conditions exist:

- When approved by the appropriate school official(s) to which the request is directed
- When authorized by the owner(s) of the information
- When required by federal, state or local law
- When required by a valid subpoena or court order

J. Assurances

1. The district makes no warranties of any kind; either expressed or implied that the functions or the services provided by or through the district system will be error-free or without defect. The district will not be responsible for any damage users may suffer, including but not limited to, loss of data or interruptions of service. The district is not responsible for the accuracy or quality of the information obtained through or stored on the system. The district will not be responsible for financial obligations arising through the unauthorized use of the system.

2. Parents or guardians will be informed of these procedures, which will be posted on the district web page.

3. These guidelines shall be submitted to the district wide Technology Steering Committee for review and approval as needed.

4. Each school will provide training in appropriate Internet and email use and rules and etiquette of acceptable use.

Questions regarding the policy or administrative procedures with respect to the use of technology and/or electronic information may be directed to the building principal.

August, 2012

Agreement to Acceptable Use Policy

Appendix 1

Student (Gr. 3-12) Acknowledgement

I have read and understand the Ballston Spa School District's Acceptable Use Policy. I understand that if I violate the rules my Internet/network access privileges can be restricted and that I may face other disciplinary measures.

Name (printed):_____

School: _____ Grade: _____

Student's Teacher (Elementary):_____

User's Signature: _____

Date: _____

Parent/guardian Acknowledgement (if applicable):

I have read and understand the Ballston Spa School District's Acceptable Use Policy and have reviewed it with my child.

Parent/guardian Signature: _____

Date: _____

Please sign and return this form to the main office.

Agreement to Acceptable Use Policy

Appendix 2

Student (Gr. K-2) Acknowledgement

Student Name (printed):_____

Grade (if applicable):_____

Student's Teacher: _____

Parent/guardian Acknowledgement:

I have read and understand the Ballston Spa School District's Acceptable Use Policy and have reviewed it with my child.

Parent/guardian Signature: _____

Date: _____

Please sign and return this form to Main Office