Acceptable Use of Electronic Information and Access

In keeping with its mission statement, the Ballston Spa Central School District is committed to providing a wide range of information technology resources to staff. Staff members have the privilege of utilizing these District owned assets.

The efficient and secure operation of technology resources relies upon the proper conduct of users. Inappropriate use exposes the District to risks including virus attacks, compromise of personal and protected data, and legal proceedings. This document is provided so that users are aware of proper conduct and responsibilities.

To be granted access to the District's technology resources, network and Internet, all individuals must read and follow the procedures outlined in this document. Faculty and staff are required to sign this document for placement in their personnel file.

All users accessing technology resources in the Ballston Spa Central School District are responsible for understanding proper procedures and rules. It is the responsibility of any user who does not understand any aspect of these procedures and rules to obtain clarification from their supervisor or the District's Technology Support Services (TSS) office.

In accordance with the Ballston Spa Central School District's policy on Staff Use of Computerized Information Resources the following requirements are established:

A. System and Data Security

Effective security is a team effort involving the participation and support of all users. The environment in which the District operates its network and online resources continues to become more complex and hostile. The following requirements are meant to address this evolving environment:

1. Users are responsible for the use of their individual account(s) and must take all reasonable precautions to prevent others from being able to access their account(s). Under no conditions should a user provide their password to another person.

2. Minimal requirements for password complexity will be provided by the District's TSS office or the appropriate system administrator.

3. Users must immediately notify their supervisor or the District's TSS office if they have noted a possible security problem. Users should not demonstrate or discuss the problem to anyone besides their supervisor or the District's TSS office.

4. Users will not download or install software or other files unless approved to do so by the District TSS office.

5. No personal devices will be connected to the District’s network without the authorization of the District’s TSS office.

6. Equipment may not be removed from District property without prior authorization.

7. Users will not disable or remove security software (e.g. DeepFreeze, anti-virus software, monitoring software, etc.) from computers.

8. Users must not open email attachments that appear suspicious or are from unknown sources. When in doubt, users should contact the District’s TSS office for assistance.

B. Confidential Information

The District is subject to multiple state and federal laws regulating its management and distribution of student and employee data. Therefore, users must be cognizant at all times of the possible confidential nature of data they are accessing and distributing.

1. Student data is protected under the Family Educational Rights and Privacy Act (FERPA) and NYS Education Law 2-d, and should not be revealed to anyone outside the requirements of these law.

2. Information related to students with Individual Education Plans is covered under the District’s policy Confidentiality & Access to Individual Education Programs. Employees with access to student IEPs must read and follow this policy.

3. Certain employee personal information is protected and should not be released. This includes information that could lead to identity theft such as social security numbers. Employees with access to employee personal data must take steps to ensure the confidentiality of this information. Questions concerning the release of employee information should be directed to the District’s Records Access Officer.

4. Data contained on portable devices such as laptops, thumb drives, smart phones, etc. are particularly vulnerable. Therefore, special precautions should be taken to protect such devices from unauthorized use. Passwords and encryption should be used where possible.

5. FERPA/Employee Personal Protected Data should not be transferred to personal devices and should not be taken off site without prior authorization of the Records Access Officer.

6. Remote Access to FERPA/Employee Personal Protected data will be strictly controlled. System administrators of information systems housing such data will provide guidelines and appropriate access restrictions.

C. Prohibited Activities

1. Under no circumstances is an employee or system user of the District authorized to engage in any activity that is illegal under local, state or federal law while using District resources.

2. Users will not attempt to gain unauthorized access to the District's system or to any other computer system through the District's system, or go beyond their authorized access. This includes attempting to log in through another person's account or access another person's files.

3. Users will not make deliberate attempts to disrupt the computer system performance or destroy data by spreading computer viruses or by any other means.

4. Users will not execute any unauthorized form of network monitoring, port scanning, or security scanning which would intercept data not intended for their use, degrade the performance of the network, or interfere with other users.

5. The illegal installation of copyrighted software or files for use on District computers is prohibited.

D. Inappropriate Communication

In utilizing the District's technology resources, employees are expected to use the same standards of acceptable conduct which apply to any aspect of job performance.

1. User restrictions against inappropriate language apply to public messages, private messages, blogs, social networks, instant messages, and material posted on web pages.

2. Users will not engage in any conduct prohibited by the District's policy on the Prohibition against Discrimination or Harassment.

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

4. All blogging should contain a disclaimer stating that the opinions expressed are strictly those of the author and not necessarily those of the District. In the course of blogging, employees are prohibited from revealing any confidential student or employee data.

5. Employees will not have frequent personal communication with a student unrelated to course work or official school matters. This applies to any form in which that personal communication may occur including, but not limited to, voice or text-based communication via phone, e-mail, instant messaging, text messaging or through social networking Web sites.

E. Respecting Resource Limits

The management of the District's technology resources is a complex and resource intensive operation. It is imperative that users understand the limited nature of these resources and utilize them in an efficient manner without diminishing other user's access.

1. Users will use the system only for educational and professional or career development activities.

2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Personal use should be limited to time periods before or after their normal workday or during break periods such as lunch.

3. Bandwidth is a shared, finite resource. Users will download large files only when absolutely necessary. If necessary, users should download approved files at a time when the system is not being heavily used.

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

5. Users will not email solicitations to other staff members for personal business purposes nor use the District's systems for personal business.

6. Faculty and staff use of email, chat, messaging, and web authoring will be used in a responsible manner. Web authoring projects will conform to the District's Internet Web Page Publication guidelines.

F. Copyright and Intellectual Property

1. Users will respect the rights of copyright owners.

2. Only legally licensed software may be installed and District computers. Software cannot be copied or installed without permission of the District's TSS office.

G. Inappropriate Access to Material

1. Users will not use the District's 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 their supervisor or the District's TSS office.

3. The District uses 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.

H. Equipment

As with any District-owned equipment, employees must take proper care of assigned IT devices and take all reasonable precautions against damage, loss, or theft. Any damage, loss, or theft must be reported immediately to the Business Office. Since employees are responsible for the safe return of District-owned IT devices, employees may be liable for damages or loss which occurs during the period of its use and/or disciplinary action.

I. Privacy and Confidentiality

The District reserves the right to inspect and examine any District owned or operated communications system, technology resource, and/or files or information contained therein at any time, without prior notice. When sources outside the District request such information, the District will follow all federal, state, or local law.

Information sent by employees via the electronic mail system may be used in legal proceedings. Electronic mail messages are considered written communications and are potentially subject to subpoena in litigation. The District will respond to subpoenas and court orders and will fulfill all legal obligations.

J. Assurances

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.

1. The District will not be responsible for any damage users may suffer, including but not limited to, loss of data or interruptions of service.

2. The District is not responsible for the accuracy or quality of the information obtained through or stored on the system.

3. The District will not be responsible for financial obligations arising through the unauthorized use of the system.

Questions regarding the policy or administrative procedures with respect to the use of technology and/or electronic information may be directed to the Assistant Superintendent of Business and Support Services. Questions about how to address specific technical issues should be directed to the TSS office.

Acceptable Use of Electronic Information and Access

User Acknowledgement

I have read and understand the Ballston Spa School District's Acceptable Use of Electronic Information and Access procedures. I understand that if I need more information about any of these procedures, I can contact the Technology Support Services office. I understand that if I violate these procedures my Internet/network access privileges can be restricted or terminated and that I may face other disciplinary measures. Disciplinary action will be implemented in accordance with employee bargaining agreements and/or applicable state law.

User's Signature: ____

User Name (printed): ____

School/Department: ____

Date: ____