Personnel

General Personnel Policies

Staff Use of Electronic Information Technology and Resources

The District positively views the appropriate use of electronic technology and resources. Electronic resources are a powerful and compelling means to enable educators to communicate, learn and share, collaborate and create, think and solve problems, and manage their work.

The District provides staff with access to electronic information technology and resources to accomplish its mission of teaching, learning and public service operations. Uses will be related to educational programs or operations of the District.

The District expects staff to use information technology and communication resources in a responsible manner in accordance with all established District policies and rules.

Acceptable network use by District staff includes:

- Creation of files, projects, videos, web pages and podcasts using network resources in support of educational research and practice.
- Participation in blogs, wikis, bulletin boards, social networking sites and groups and the creation of content for podcasts, e-mail and web pages that support educational research and practice.
- The online publication of original educational material, curriculum related materials and student work. Sources outside the classroom or school must be cited appropriately.
- Connection of staff personal laptops to the district network after checking with the Information Technology and Network Specialist to confirm that the laptop is equipped with up-to-date virus software, compatible network card and is configured properly. Connection of any personal electronic device is subject to all guidelines in this document.

Unacceptable network use by District staff includes but is not limited to:

- Personal gain, commercial solicitation and compensation of any kind.
- Liability or cost incurred by the district.
- Downloading, installation and use of games, audio files video files or other applications (including shareware or freeware).
- Support or opposition for ballot measures, candidates and any other political activity unless it is related to a curricular goal in an appropriate course.
- Hacking, cracking, vandalizing, the introduction of viruses, worms, Trojan horses, time bombs and changes to hardware, software, and monitoring tools.
- Unauthorized access to other district computers, networks and information systems;
- Cyberbullying, hate mail, defamation, harassment of any kind, discriminatory jokes and remarks;
- Information posted, sent or stored online that could endanger others (e.g., bomb construction, drug manufacture);.
- Accessing, uploading, downloading, storage and distribution of obscene, pornographic or sexually explicit material.

- Attaching unauthorized equipment to the district network. Any such equipment will be confiscated and destroyed.

Discipline

Use of such resources for unacceptable purposes may be cause for discipline up to and including termination, consistent with applicable employee handbook and/or District policy. The District shall cooperate with legitimate law enforcement investigations.

Electronic communication use is subject to many of the same statutes and legal requirements as other forms of communication. All such documents are generally considered to be public records and are subject to public inspection. To the greatest extent possible in a public setting, individuals' privacy will be preserved. However, communication across District networks should not be considered private. Privacy in these communications is not guaranteed. Although the District does not make a practice of monitoring individual messages, access to information, or use of equipment, the Superintendent/designee is authorized to access and review such usage and reserves the right to retrieve the content for legitimate reasons. The District shall take appropriate corrective action or disciplinary action against an employee based upon information obtained from monitoring or inspecting his/her District equipment, electronic records and communications. The District's practice of not monitoring every communication is not a waiver of its right to monitor in the future. All employer-issued equipment and all data generated, received or stored on such equipment is the property of the District. The District retains the right to confiscate any District-owned equipment at any time.

The Superintendent/designee shall specify those behaviors that are permitted and those that are not permitted, as well as appropriate procedures to guide employee use. In general, employees are expected to communicate in a professional manner consistent with District policy and guidelines, as well as with, State and federal laws.

Personally Owned Technology/Software

Installation and use of personal software on District computers is generally prohibited due to assuring District compliance with software copyright issues. The District is in no way obligated to provide service on personal equipment. In the event that the District deems it in their best interest to provide such service, the District shall not be held liable or responsible for any potential repairs that may have been caused by such service. Staff may connect their personal devices to the District's network, however, any information sent over the District's network will be monitored and staff should not expect any privacy on information sent utilizing the District's network.

Staff use of Information Technology and Communication Resources

Users of electronic communication systems shall be aware that, in addition to being subject to authorized access, communication in its present form cannot be secured and is, therefore, vulnerable to unauthorized access and modification by third parties. Receivers of electronic documents shall check with the purported sender if there is any doubt about the identity of the sender of the authenticity of the contents, as they would with print documents. Users of the District's electronic mail services shall be aware that even though the sender and recipient have discarded their copies of an electronic record, there may be back-up copies that can be retrieved.

The District shall not be liable for an employee's inappropriate use of the electronic communication system or violations of copyright restrictions, employees' mistakes or negligence, or costs incurred by employees. The District shall not be responsible for ensuring the accuracy of usability of any information sent during electronic communications. Views or opinions presented in electronic communications are solely those of the employee and do not necessarily represent those of the District.

All communications transmitted over the District's network or otherwise made in the course of business are governed by the District's Harassment and Equal Employment Opportunity policies. Policy or rule violations shall result in appropriate disciplinary action up to and including termination and/or legal action, if warranted. The District shall cooperate fully with local, State, or federal officials in any investigation concerning or relating to misuse of the District's electronic communications system.

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. Requests may be made to have instructionally useful sites unblocked. It is expected that the classroom teacher has reviewed content of such sites for their instructional appropriateness.

- 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 appropriate 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: 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.
- 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.
- Staff must make a reasonable effort to become familiar with the Internet and to monitor, supervise, instruct and assist 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

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. 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 on a regular basis (no less than twice yearly).
- Do not use another user's account.
- Do not insert passwords into e-mail or other communications.
- If you write down your account password, keep it out of sight.
- Do not store passwords in a file without encryption.
- Do not use the "remember password" feature of Internet browsers.
- 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.
- Any and all information transmitted or received in connection with network and e-mail use.

No employee 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 Wisconsin.

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 according to a timetable set by the Information Technology and Network Specialist. The District is not responsible for files residing on non-district servers.

Confidentiality of Staff an Student Information and Data

The District expects all staff to follow confidentiality policies and laws when handling and working with student and staff information and data.

Legal Reference: **Federal Copyright Law**
Children's Internet Protection Act
Family Education Rights and Privacy Act
Wisconsin Statute – Chapter 19
Wisconsin Statute – 943.70
Wisconsin Statute – 947.0125

Policy Approved: **July 27, 2015**

Policy Revised: