STAFF USE OF INFORMATION TECHNOLOGY AND COMMUNICATION RESOURCES

The District provides staff with access to information technology and communication resources to accomplish its mission of educating students, and use of same shall be carried out in a responsible manner in accordance with established Board policies and rules outlined in the *Employee Handbook*. Among the resources within the scope of this policy and its implementing rules are the following: internet, telephones (including cell phones and the voicemail system), technology devices (whether used on or off campus), fax machines, digital communications (including email), wireless access points, printers, cameras, removable storage devices, and any other device or equipment that the District reasonably deems to fall within the scope of this policy.

Users of District information technology and communications resources shall have no expectation of privacy with respect to such use. Consequently, all software, email, voicemail, files, digital communications, and other information or documents used, generated, transmitted or received over District data, voice or video networks, or stored on District equipment, are the property of the District. The District retains the right to review, monitor, audit, intercept, access and disclose all messages or information created, received or sent over District data, voice or video networks, or stored on its equipment. Additionally, email messages, text messages, and other documents created or received by staff may be subject to release in accordance with applicable public records law.

The administration shall create and enforce rules for use of information technology and communication resources. Policy or rule violations may result in one or more of the following: (1) restriction of access to District information technology and communication resources; (2) appropriate disciplinary action, up to and including discharge; and (3) referral of the matter to law enforcement authorities. At all times, staff should be aware that use of District resources is a privilege, not a right, and that privilege may be restricted or revoked at any time.

ADOPTED: March 14, 2018

REVISED:

REVIEW DATE: March 14, 2018

LEGAL REFERENCES:

Wisconsin Statutes

Sections 19.31 to 19.37	[Wisconsin Public Records Law]
Sections 19.62 - 19.80	[personal information practices]
Section 120.12(1)	[school board duty; care, control and management of school district property]
Section 120.44(2)	[school board duties and powers; unified school districts]
Section 943.70	[computer crimes]
Section 947.0125	[unlawful use of computerized communication systems]
Section 995.55	[access to personal Internet account information]

Wisconsin Administrative Code:

ADM 12	[electronic records management]

Federal Laws:

Children's Internet Protection Act	[Internet safety policy required, which includes protections against Internet access to visual depictions that are obscene, child pornography and material harmful to children]
Title 17 U.S.C.	[use and copying of copyrighted materials, including "fair use"] Electronic Communications Privacy Act [I 8 U.S.C. §§ 2510-22]
CROSS REFERENCES:	GBCD-R, Staff Use of Information Technology and Communication Resources Rules GBCD-E, Acknowledgement of Acceptable Use of Technology Rules BY STAFF/USERS Employee Handbook

STAFF USE OF INFORMATION TECHNOLOGY AND COMMUNICATION RESOURCES RULES

District employees are expected to abide by the following rules when using information technology and communication resources:

A. Electronic Communications:

1. Electronic communications are protected by the same laws and policies and are subject to the same limitations as other types of media. When creating, using or storing messages on the network, the user should consider both the personal ramifications and the impact on the District should the messages be disclosed or released to other parties. Extreme caution should be used when committing confidential information to the electronic messages, as confidentiality cannot be guaranteed.

2. The District may review email logs and/or messages at its discretion. Because all technology devices hardware, digital communication devices and software belong to the District, users have no reasonable expectation of privacy, including the use of email, text-message and other forms of digital communications, e.g. voicemail, Twitter™, Facebook™, etc. except as noted herein. The District may through such review of email logs and/or messages inadvertently obtain access information for an employee's personal internet account through the use of an electronic device or program that monitors the District's network or through an electronic communications device supplied or paid for in whole or in part by the employer. If such personal internet access information is obtained by the District, the District shall not use that access information to access the employee's personal internet account unless permitted by law.

3. The use of the District's technology and electronic resources is a privilege which may be revoked at any time.

4. Electronic mail transmissions and other use of the District's electronic communications systems or devices by employees shall not be considered confidential and may be monitored at any time by the Superintendent or his designee to ensure appropriate use. This monitoring may include, but is not limited by enumeration to, activity logging, virus scanning, and content scanning. Participation in computer-mediated conversation/discussion forums for instructional purposes must be approved by curriculum or District administration. External electronic storage devices are subject to monitoring if used with District resources.

B. User Responsibilities: Network/Internet users, like traditional library users or those participating in field trips, are responsible for their actions in accessing available resources. The following standards will apply to all users of the network/Internet:

1. The user, in whose name a system account is issued, will be responsible at all times for its proper use. Users may not access another person's account without written permission from an administrator or immediate supervisor. All employees must sign an Acceptable Use Policy (AUP) as a condition of employment and as needed for any AUP reasons.

2. The system may not be used for illegal purposes, in support of illegal activities, or for any other activity prohibited by District policy.

3. Users may not redistribute copyrighted programs or data without the written permission of the copyright holder or designee. Such permission must be specified in the document or must be obtained directly from the copyright holder or designee in accordance with applicable copyright laws, District policy, and administrative regulations.

4. A user must not knowingly attempt to access educationally inappropriate material. If a user accidentally reaches such material, the user must immediately back out of the area on the Internet containing educationally inappropriate material. The user must then notify the building principal and/or immediate supervisor of the site address that should be added to the filtering software, so that it can be removed from accessibility. The building principal and/or supervisor shall log the incident.

5. A user may not disable Internet tracking software or implement a private browsing feature on District computers or networks. Browsing history shall only be deleted by authorized staff or in accordance with the District's technology department's directives. Deleting browsing history from a local workstation using the district provided Internet navigation software is allowed.

C. Electronic Communications with Students: Employees are prohibited from communicating with students who are enrolled in the District through electronic media, except as set forth herein. An employee is not subject to this prohibition to the extent the employee has a pre-existing social or family relationship with the student. For example, an employee may have a pre-existing relationship with a niece or nephew, a student who is the child of an adult friend, a student who is a friend of the employee's child, or a member or participant in the same civic, social, recreational, or religious organization. The following definitions apply for purposes of this administrative rule:

- "Authorized Personnel" includes classroom teachers, counselors, principals, assistant principals, directors of instruction, coaches, athletic director, athletic trainers, club/activity supervisor, and any other employee designated in writing by the District Administrator or a building principal.

- "Communicate" means to convey information and includes a one-way communication as well as a dialogue between two or more people. A public communication by an employee that is not targeted at students (e.g., a posting on the employee's personal social network page or a blog) is not a communication; however, the employee may be subject to District regulations on personal electronic communications. Unsolicited contact from a student through electronic means is not a communication.

- "Electronic media" includes all forms of social media, such as, but not limited by enumeration to, the following: text messaging, instant messaging, electronic mail (email), Web logs (blogs), electronic forums (chat rooms), video sharing Websites (e.g., YouTube™), editorial comments posted on the Internet, and social network sites (e.g., Facebook™, Instagram™, Twitter™, LinkedIn™), and all forms of telecommunication such as landlines, cell phones, and web-based applications.

D. Limited Electronic Communication with Students: Employees may communicate through electronic media with students who are currently enrolled in the District only within the following guidelines:

1. The employee shall limit communications to matters within the scope of the employee's professional responsibilities (e.g., matters relating to class work, homework, field trips, tests, practice/game times, transportation).

2. If an employee receives an unsolicited electronic contact from a student that is not within the employee's professional responsibilities (e.g., for classroom teachers, items such as matters relating to class work, homework, and tests), the employee shall not respond to the student using any electronic media except to address a health or safety emergency.

3. The employee is prohibited from communicating with students through a personal social network page; the employee must create a separate social network page ("professional page") for this purpose. The employee must enable administration and parents to access the employee's professional page.

4. Upon request from the administration, an employee will provide the phone number(s), social network site(s), or other information regarding the method(s) of electronic media the employee uses to communicate with any one or more currently-enrolled students.

5. The employee continues to be subject to applicable state and federal laws, local policies, and administrative regulations.

E. Retention of Electronic Communications and other Electronic Media: The District archives all non-spam emails sent and/or received on the system in accordance with the District's adopted record retention schedule. After the set time has elapsed, email communications may be discarded unless the records may be relevant to any pending litigation, pending public records request, or other good cause exists for retaining email records. The Wisconsin Department of Public Education Retention Schedule is provided here. Additionally, access Board Policy KBG regarding Access to Public Records.

   Employees who create student records via email need to ensure that student records are retained for the period of time specified by the student records law. For this reason, the District heavily discourages the use of email as the means to communicate about individually identifiable students.

F. Compliance with Laws and Local Policies and Regulations: For all electronic media, employees are subject to certain state and federal laws, local policies, and administrative regulations, even when communicating regarding personal and private matters, regardless of whether the employee is using private or public equipment, on or off District property. These restrictions include:

   1. Confidentiality of student records. Reference Board Policy JO.

   2. Confidentiality of other District records, including staff evaluations, and private email addresses.

   3. Confidentiality of health or personnel information concerning colleagues, unless disclosure serves lawful professional purposes or is required by law.

   4. Prohibition against harming others by knowingly making false statements about another employee or the District.

5. Prohibitions against soliciting or engaging in sexual conduct or a romantic relationship with a student.

6. Upon written request from a parent, the employee shall discontinue communicating with the parent's minor student through email, text messaging, instant messaging, or any other form of one-to-one communication.

7. An employee may request an exception from one or more of the limitations above by submitting a written request to his/her immediate supervisor.

G. Personal Web Pages**:** Employees may not misrepresent the District by creating, or posting any content to, any personal or non-authorized website that purports to be an official/authorized website of the District. No employee may purport to speak on behalf of the District through any personal or other non-authorized website.

H. Personal Electronic Devices: All staff must use the guest network. The District permits staff to use personal technology devices in support of teaching and learning and to access the District's Wireless Public Network when doing so. Personal devices include laptop computers, portable digital assistants (PDAs), cell phones, smart phones, iPods/MP3 players, wireless devices, digital cameras, e-readers, storage devices, or other electronics that may be carried on a person. Staff may use personal devices provided such use does not interfere with educational or employment responsibilities, hinder, disrupt or consume an unreasonable amount of network or staff resources, or violate board policy, administrative rules, state law or federal law. An employee using a personal device shall take adequate measures to ensure the confidentiality and proper maintenance of all student record information. The District is not liable for the loss, damage or misuse of any personal device including while on District property or while attending school-sponsored activities.

I. Disclaimer: The District's electronic systems are provided on an "as is, as available" basis. The District does not make any warranties, whether expressed or implied, including, without limitation, those of merchantability and fitness for a particular purpose with respect to any services provided by the system and any information or software contained therein. The District does not warrant that the functions or services performed by, or that the information or software contained on the system will meet the system user's requirements, or that the system will be uninterrupted or error-free, or that defects will be corrected. Opinions, advice, services, and all other information expressed by system users, information providers, service providers, or other third-party individuals in the systems are those of the individual or entity and not the District. The District will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the District's electronic communications system.

3/14/18

ACKNOWLEDGEMENT OF ACCEPTABLE USE OF TECHNOLOGY RULES BY STAFF/USERS

SCHOOL YEAR: _____

The use of the District's Information Technology Systems, including the Internet, may be provided for your professional use. You are required by the School District of Jefferson to sign this form, acknowledging your responsibilities for this resource prior to gaining access to the District's system and equipment.

Staff/User's Name:_____

Position:_____

School or Department:_____

I have received, read and fully understand the School District of Jefferson's **STAFF USE OF INFORMATION TECHNOLOGY AND COMMUNICATION RESOUCES RULES**.

I agree to comply with the policy as a condition of my employment with the School District of Jefferson or access to the District's systems.

I understand that a violation of the **STAFF USE OF INFORMATION TECHNOLOGY AND COMMUNICATION RESOUCES RULES** policy may result in disciplinary action, up to and including discharge, and/or appropriate legal action.

Staff/User's Signature: _____**Date**: _____

3/14/18