STAFF/USERS INFORMATION TECHNOLOGY SYSTEMS ACCEPTABLE USE POLICY

The School District of Jefferson, referred herein as "SDOJ" or "District," provides staff and/or users with access to the District's Information Technology systems for educational and business purposes in order accomplish the mission of educating students in conformance with applicable law.

The District's Information Technology (IT) systems connect to the district network or access district applications. Information Technology system refers to, but is not limited to, the District's Internet, intranet, e-mail, telephone, computer equipment and computer systems (collectively referred to as the "Systems"). The District provides access to the Systems to support the educational mission of the schools, enhance the curriculum and learning opportunities for students and school users, increase communication within the District, enhance productivity and assist users in improving school and student outcomes. The School Board has established this policy and its guidelines to ensure appropriate use of these resources.

ADOPTED: March 17, 1997 [under Computer Acceptable Use Procedures (AUP)]
March 18, 2002 [under Policy IIBG]

REVISED: April 24, 2000 [under Computer Acceptable Use Procedures (AUP)]
June 8, 2009
June 22, 2015

REVIEW DATE: June 22, 2015

LEGAL REF.: Wisconsin Statutes: 120.44(2) 943.70 947.0125 995.55
Children's Internet Protection Act (CIPA) (Title XVII of the FY2001 Labor-HSS Appropriations Act, Pub. L. No. 106-554 [2000])

CROSS REF.: IIBG-R, Staff/Users Information Technology Systems Acceptable Use Policy Guidelines

IIBG-E, Staff/Users Information Technology Systems Acceptable Use Agreement

School District of Jefferson Employee Handbook

ACA, Employee Harassment Policy

ACB, Student Harassment Policy

STAFF/USERS INFORMATION TECHNOLOGY SYSTEMS ACCEPTABLE USE POLICY GUIDELINES

GUIDELINES

1. **Responsibilities Related to Technology System Management and Training**
    a. The District's Technology Coordinator works with the Information Technology Director and Technology Integrator to manage, maintain and improve the District Technology Systems.
    b. The District's Technology Coordinator and Technology Integrator serve as the coordinators to ensure users receive proper training in the use of the Systems and the requirements of this Policy and Guidelines.
    c. Staff will actively monitor students who are engaged in online learning activities.
    d. Users will preview the materials and sites they require or recommend students access to determine the appropriateness of the material contained on or accessed through the site.
    e. The District shall maintain an Internet filtering measure that blocks access to the three categories of visual depictions specified by the Children's Internet Protection Act—obscene material, child pornography, and material that is deemed harmful to minors. The District may, in its discretion, disable such filtering for certain users for District-approved research or other lawful educational and business purposes.

2. **Access to Information Technology Systems and Internet Services**
    a. The level of access users have to the School District of Jefferson's computers, networks, and Internet services is based upon specific user's job requirements and/or needs.
    b. A current, signed *Staff/Users Information Technology Systems Acceptable Use Agreement* must be on file with the IT Department prior to system access being granted to any user.

3. **Acceptable Use**
    a. User use of the computer network may be electronically monitored. The district reserves the right to monitor, access, remove and disclose any message or document created, archived, stored, received, deleted, looked at or sent with the District's computer network, without prior notice to user. Users suspected of inappropriate or prohibited system use will be investigated. Users must immediately disclose to their supervisor or building administrator any messages they received that are inappropriate or that make them feel uncomfortable.
    b. The Systems are to be used for educational and professional development activities. Limited personal use of the Systems is permitted during non-instructional or non-supervisory time; excessive personal use of the Systems may result in disciplinary actions.
    c. To respect resource limits and promote equitable sharing of resources, users are not to monopolize or abuse access to the Systems by, among other possibilities, storing an excessive amount of information or using the Systems for unauthorized purposes.

4. Social Networking

a. The use of online social networking sites where users can create customized profiles and/or form connections with other users based on shared characteristics and interests such as chat rooms, wikis, blogs, forums and other applications will be allowed online in controlled, administrator-supervised settings, and for valid school-related purposes. All other purposes are prohibited.
b. Users wishing to establish a school-sponsored social network site must get approval from the building principal and district technology coordinator. The site must hold a direct educational value to the sponsoring SDOJ grade level, department, or activity. The user will become the site coordinator and must be able to provide account details to the building principal and district technology coordinator upon request. The site coordinator will become solely responsible for adding participants to the social network site and will be responsible for educating the student participants on appropriate use of the site.
c. Users may not post confidential or otherwise legally protected information or materials on any online forum.
d. Users shall only communicate electronically with students for which they have instructional, supervisory, or safety check responsibilities. The user shall limit communications to matters within the scope of the user's professional responsibilities. For classroom teachers, this refers to homework and tests. For coaches and trainers, this refers to matters related to extracurricular purposes.

5. Unauthorized Activities

a. Users will not attempt to gain unauthorized access to the Systems or any other computer system through the Systems, or go beyond their authorized access. This includes attempting to log in through another person's account or accessing another person's files.
b. Users will not install ANY software on the local hard drive of District computers, including, but not limited to, games, chat clients, e-mail clients, instant messaging, and other non-authorized applications or utilities, without the expressed permission of the Information Technology Director/Department. Users will not alter any software configuration that is stored on a workstation.
c. Users will not make deliberate attempts to disrupt the District's Technology Systems' performance or destroy data by intentionally spreading computer viruses or by any other means.
d. Users will not attempt to delete, erase or otherwise conceal any information stored on a school computer or use the District's Systems to engage in any illegal act or other action that violates Board Policy.
e. Users will not use the District's Systems to engage in political campaigning or personal commercial purposes.

6. System Security

a. Users are responsible for the use of their individual accounts and should take all reasonable precautions to prevent others from being able to use their personal accounts. Under no conditions should a user provide his/her password to another person.

b. Users will immediately notify the District's IT Director/Department if they have identified a possible security problem. Users will not search for security problems because this may be construed as an unauthorized attempt to gain access to the Systems.

7. Privacy

a. Electronic files created, sent, received, or stored on SDOJ owned, leased, administered, or otherwise under the custody and control of SDOJ are the property of SDOJ and user use of these such files is neither personal nor private except where required to do so by local laws.
b. District users must recognize that electronic files and communications may be public records subject to state open records requirements, and they must take appropriate actions to maintain such records are in compliance with state law.

8. Inappropriate Language, Harassment, and Cyberbullying

a. Restrictions against inappropriate language apply to public messages, private messages, and material posted on webpages and social media.
b. Users will not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening or disrespectful language.
c. Users will not post information that, if acted upon, could endanger the health, safety, or welfare of other individuals.
d. Users will not engage in personal attacks including, but not limited to, prejudicial or discriminatory attacks.
e. Users will not harass or bully another person. Harassment is defined as "any act or attempted act intended to cause physical injury, or emotional suffering or property damage through intimidation, stress, humiliation, bigoted epitaphs, vandalism, force or threat of any of the above, motivated by, but not limited to hostility towards the victim's real or perceived sex, race, color, religion, national origin, ancestry, creed, pregnancy, marital status, sexual orientation, disability/handicap, or any other basis protected by state or federal law."
f. Users will not engage in cyberbullying. Cyberbullying is defined as "The use of information and/or communication technologies such as, but not limited to, e-mail, cell phone and text messages, social networking sites, video posting sites, instant messaging, defamatory personal websites, and defamatory online personal polling websites, to support deliberate, repeated, and hostile behavior by an individual or group that is intended to harm others." In situations whereby cyberbullying originated from a non-school computer or other communication devices (i.e., smartphone) and is brought to the attention of the building administration, any disciplinary action taken shall be based upon whether the conduct is determined to be substantially disruptive of the educational process so that it markedly interrupts or substantially impedes the day-to-day operations of a school. Such conduct includes, but is not limited, to harassment or making a threat off school grounds that is intended to endanger the health, safety or property of others at school or at a school related activity wherever held, or toward a District employee or School Board member.

9. Plagiarism and Copyright Infringement

a. Users shall not plagiarize or infringe on the copyrights or trademarks of any work, including works found on the Internet. Users shall be held personally liable for any of their own actions that violate copyright laws. All sources must be cited.

10. Use of Personal Technology and Devices

a. A personally-owned computer or communications device may be connected to the Internet only through the District's public wireless network (eagleguest), which allows filtered web-only access to the Internet. Personal devices are never to be physically plugged into a network drop or connected to the district private wireless network.
b. Personal technology and devices (i.e., laptops, tablets, smartphones, etc.) are not managed or supported by the district. Users are solely responsible for any personal device that they bring on District property.
c. Users are not required to bring personal electronic property to school. The District accepts no responsibility for the loss, theft, or damage of personal property brought to school by the user. Any personal technology brought to school is the sole responsibility of the user bringing the device to school.

11. Policy and Rule Violations

a. For all electronic media, users are subject to certain state and federal laws, local policies, and school guidelines, regardless of whether the user is using public or private equipment, on or off District property. These restrictions include:
    i. Confidentiality of student records
    ii. Confidentiality of other District records, including educator evaluations and private e-mail addresses.
    iii. Confidentiality of health or personal information concerning users, unless disclosure serves lawful professional purposes or is required by law.
    iv. Prohibition against harming others by knowingly making false statements about a colleague, student, or the District.
    v. Prohibitions against soliciting or engaging in sexual conduct or a romantic relationship with a student.
b. Failure to comply with Board policies regarding user's use of the District's Technology Systems, including the use of the Internet, may result in disciplinary action, up to and including discharge.
c. Illegal use of the District's Technology Systems, including the use of the Internet, will result in referral to law enforcement authorities.

6/22/15

STAFF/USERS INFORMATION TECHNOLOGY SYSTEMS ACCEPTABLE USE AGREEMENT

Acknowledgement of Consent and Acceptance of Policies, Rules, and Procedures

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/USERS INFORMATION TECHNOLOGY SYSTEMS ACCEPTABLE USE POLICY AND GUIDELINES. 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 Acceptable Use policy may result in disciplinary action, up to and including discharge, and/or appropriate legal action.

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

6/22/15