SCHOOL DISTRICT OF JEFFERSON
BOARD OF EDUCATION POLICY

Reference Code: IIBH

STUDENT INFORMATION TECHNOLOGY SYSTEMS ACCEPTABLE USE POLICY

The School District of Jefferson, referred herein as "SDOJ" or "District," provides students with access to the District's Technology Systems which means all Information Technology (IT) that connects to the District Network or accesses District applications. This includes, but is not limited to, the District's Internet, e-mail, computer equipment, and computer systems (collectively referred to as the "Systems"). The District provides students with networked devices (computers, tablets, etc.) as a means to further educational goals and objectives of the District. The School Board has established this acceptable use policy and its guidelines to ensure appropriate use of these resources.

ADOPTED: June 22, 2015

REVISED:

REVIEW DATE: June 22, 2015

LEGAL REF.: Wisconsin Statutes: 120.13(1) 120.44(2) 943.70 947.0125 995.55
Public Law No: 110-385 Title II Protecting Children in the 21st Century Act

Children's Internet Protection Act (CIPA) (Title XVII of the FY2001 Labor-HSS Appropriations Act, Pub. L. No. 106-554 [2000])

CROSS REF.: IIBH-R, Student Information Technology Systems Acceptable Use Policy Guidelines

IIBH-E, Student Information Technology Systems Acceptable Use Agreement

ACB, Student Harassment Policy

STUDENT 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 staff and students 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. Teachers 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 bona-fide research or other lawful educational and business purposes.

2. **Access to Information Technology Systems and Internet Services**
    a. The primary purpose of providing access to the Systems is to enhance learning, thereby better preparing students for success in life and work. In addition, this access is provided to increase communication and collaboration among students and their teachers.
    b. Access to the Systems by students requires adherence to the District *Student Information Technology Systems Acceptable Use Policy and Guidelines*. Each student wishing to use the District's Information Technology resources and Internet services shall have a parent signature on file (electronic or on paper) and will be expected to abide by the established policy and guidelines. This agreement is valid for the time the student attends a particular school (i.e., elementary, middle school, high school).

3. **Acceptable Use**
    a. Student 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 Systems, without prior notice to users. Students suspected of inappropriate or prohibited computer network use will be investigated.
    b. Students must immediately disclose to their teacher any messages they received that are inappropriate or that make them feel uncomfortable.

4. **Social Networking**
    a. The use of online social networking sites where users can create customized profiles and form connections with other users based on shared characteristics and interests such as chat rooms,

snapchat, wikis, blogs, forums, will be allowed in controlled, staff-supervised settings, and for valid school-related purposes. All other uses are prohibited.

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 download and/or install software or alter any software configuration that is stored on a computer, tablet, or device.
c. Users will not make deliberate attempts to disrupt the District's Information Technology Systems' performance or destroy data by intentionally spreading computer viruses or by any other means.
d. Users will not use the District Information Technology Systems to engage in any illegal act or other action that violates any other Board Policy.
e. Online game playing, music downloads and streaming, video downloads and streaming, and online gambling, unless used to gather educational materials for classroom instruction, is strictly prohibited.

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, including logging off after their network session has ended. Under no conditions should a user provide his/her password to another person, use another person's username and password, or use an unattended machine logged on under another individual's username.
b. Users will immediately notify the supervising teacher (without showing other users) if they have identified a possible security problem (i.e., being able to access other user's data).
c. Users will not search for security problems because this may be construed as an unauthorized attempt to gain access (i.e., computer hacking).

7. Privacy

a. Electronic files created, sent, received, or stored on equipment owned, leased, administered, or otherwise under the custody and control of SDOJ are the property of SDOJ and student use of such files is neither personal nor private except where required to do so by local laws.

8. Inappropriate Language, Harassment, and Cyberbullying

a. Users will not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language.
b. Users will not post information that, if acted upon, could endanger the health, safety or welfare of other individuals.
c. Users will not engage in personal attacks including, but not limited to, prejudicial or discriminatory attacks.
d. 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."

e. 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 in which cyberbullying originated from a non-school computer or other communication devices (i.e., smartphone) and is brought to the attention of 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. Students shall comply with legal requirements regarding the use, reproduction, and distribution of copyrighted works. Teachers will instruct students in appropriate research and citation practices.

10. Use of Personal Technology and Devices

a. Students may use personally owned devices as allowed by building policy.
b. 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's private wireless network.
c. Personal technology and devices (i.e., laptops, tablets, smartphones, etc.) are not managed or supported by the district. Students are solely responsible for any personal device that they bring on District property.
d. 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 a student. Any personal technology brought to school is the sole responsibility of the student bringing the device to school.

11. Policy and Rule Violations

a. Student use of the Information Technology system shall be viewed as a privilege, not a right. Information technology resources may be used for educational research, communication and collaboration purposes consistent with the educational goals and objectives of the District. Misuse of Information Technology resources may result in the suspension of use privileges and/or school disciplinary action. Use of any of SDOJ's resources for any illegal activity will be subject to appropriate disciplinary action and the District will not hesitate to cooperate with any criminal investigation and prosecution that may result from such activity.

STUDENT INFORMATION TECHNOLOGY SYSTEMS ACCEPTABLE USE AGREEMENT

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

SCHOOL YEAR:_____

PARENT CONSENT

Information Technology Systems and Internet Access

I have read and understand that my child must abide by the School District of Jefferson Acceptable Use Policy. I recognize it is impossible for the District to restrict access to all controversial materials, and I will not hold the school responsible for materials acquired on the school network. I understand that children's computer activities at home should be supervised as they can affect the academic environment at school.

I hereby give permission for my child to use the School District of Jefferson's computer resources, including Web- or Internet-based services provided by other companies or institutions which have been approved by the SDOJ for student use. I understand that my child's Internet activities will be monitored by the District, and any violation may result in the suspension or termination of technology system privileges and will be subject to appropriate disciplinary action and/or prosecution.

Parent Signature:_____ Date:_____

Students without a signed form on file may be denied access to resources, including login and password information.

9/26/16