ACCEPTABLE USE OF TECHNOLOGY

This Policy sets forth basic guidelines that all students and employees of the District are expected to follow when using any District-owned network or device (as defined below). The district is not responsible for systems or networks over which it has no control. Parents and/or guardians of minors are responsible for setting and conveying the standards that their children should follow when using these electronic resources and online environments at home. Failure to abide by District policy and administrative regulations governing the use of these resources may result in the suspension and/or revocation of system access. Additionally, any student violation may result in discipline up to and including expulsion. Staff violations may also result in discipline up to and including dismissal.

Copies of this Policy shall be posted on the District's web site, will be made available in all building and District offices, and will be made available electronically to all District staff, students, and parents.

All users must agree to the Acceptable Use Policy Agreement before accessing any Iowa City Community School District (ICCSD) Network Resources.

DISTRICT OWNERSHIP

The District, at its sole discretion, may provide access to various technological resources, including but not limited to the Internet and the District's network, District email, web resources and platforms, computing devices (including desktop computers, laptop computers, and tablets and all peripheral devices thereto) to employees and students. The District may also, at its sole discretion, provide employees with access to District voicemail, cell phones, and/or smart phones as necessary to perform their job duties. Collectively, these resources will be referred to as the District's "Network Resources."

The District provides these Network Resources as a benefit to students and employees for the sole purpose of enhancing the educational opportunities offered by the District. Use of all ICCSD Network Resources is a privilege and not a right.

NO EXPECTATION OF PRIVACY

ICCSD is a public entity, therefore, all records (except those specifically excluded by law), whether in electronic or hardcopy form, are subject to the Freedom of Information Act and open to public inspection.

All of the District's Network Resources are District property and are not confidential. The District has the right to access, review, copy, modify, and delete any information transmitted through or stored in the District's systems or devices, including but not limited to email, web postings, text messages, and other electronic communications. Files containing personal information about a student or employee that are transmitted through or stored in the District's systems or devices are treated no differently that the District's other files, and students and employees have no expectation of privacy in such materials.

All communications sent over the ICCSD network or to or from any ICCSD-provided account or device, including text and images, may be subject to disclosure to applicable law enforcement or other third parties without prior consent of the sender or the receiver, as provided by law.

USER'S RESPONSIBILITY

Users shall be responsible for the proper use of all ICCSD Network Resources issued or made available to them by the District. Students are responsible for immediately notifying a staff member of any damage to the device that they are using. Employees must immediately report any damage to their own District-issued devices to their building principal, district technology staff, or to a district administrator.

NETWORK SECURITY AND SAFETY

To the extent required by federal law, the District shall use technology protection measures to protect against the access of inappropriate materials online.

The District will monitor the online activities of students and will provide age-appropriate education and training about the provisions of this policy, including safe and appropriate online behavior (including interaction on social networking sites and chat rooms) and cyberbullying awareness and response.

All users must follow these guidelines for promoting network security and safety:

- Users shall not share their account with anyone or leave the account open or unattended.
- Passwords shall remain confidential and should be protected by the user and not shared or displayed.
- Users are responsible for immediately notifying District technology staff or administration of any possible security problems.
- For personal safety reasons, users should never reveal their full name, address or location, telephone number, or any other personally identifiable information to unknown parties using District Network Resources. Students should only communicate with others online using District Network Resources for educational purposes. Students should **never** share personally identifiable information or arrange a meeting in person with an individual whom they met online.
- Users should immediately inform a building or district administrator of any online communication that is threatening, harassing, or otherwise inappropriate.

ACCEPTABLE USES OF TECHNOLOGY

I. Responsible Use

A. The authority for monitoring acceptable use of electronic Internet resources is delegated to ICCSD staff members assigned to classrooms and the technology department.
B. Instruction in the proper use of the Internet will be provided to staff members who will then provide similar instruction to students.
C. Students and staff members are expected to practice appropriate use of the Internet, including compliance with applicable laws and District policies. Violations may result in disciplinary action.
D. The smooth operation of the network relies upon the proper conduct of the users who must adhere to strict guidelines that require efficient, ethical and legal utilization of the computer network.
E. Users are responsible for the content of all text, audio or images that they place on or send over the Internet.
F. If a student gains access to any service via the Internet which has a cost involved, or if a student incurs other types of costs, the student accessing such a service will be responsible for those costs.
G. Any use of the Internet or transmission of material, information or software in violation of any federal, state, or local law or regulation, board policy, or building regulation is prohibited.

II. Rules Applicable to Specific Network Resources

1. Internet

A. The Internet may be used by students and staff for school appropriate research or reference, or other legitimate educational purposes.
B. Users should attempt to access only school-appropriate material when using search engines such as Google, Bing, etc. to find web sites, images, or files.
C. Should users encounter inappropriate material by accident, they should leave the site immediately.

2. E-Mail

All users of district email accounts must adhere to the following guidelines:

A. Use of objectionable language is prohibited.
B. Always use caution when addressing messages to ensure that messages are not inadvertently sent to the wrong party.
C. Transmission, creation, or access of bullying or harassing, defamatory, obscene, pornographic, profane, offensive, threatening, or discriminatory messages or messages that disclose personal or confidential information without authorization is strictly prohibited.
D. Use of the ICCSD Network or ICCSD-provided accounts or devices to improperly distribute copyrighted materials is prohibited.
E. Passwords must not be written down and shall not be shared with anyone. Any employee identified as a security risk or having a history of problems with

information security may be denied access to the ICCSD Network and ICCSD-provided accounts and/or devices.

F. Use of another's user name/account to access email, internet, or other online resources with or without that user's permission, is strictly prohibited.

3. Computers, Laptops, Tables, and Other Similar Devices

A. Users should log in using their own username. Use of another's username and password, with or without that user's permission, is strictly prohibited.
B. Users must handle all physical components of the computing or communication device with care, including all peripherals. Keyboards and mice should be kept with computer workstations and not moved.

4. Cell Phones, Smart Phones, and Other Handheld Devices

A. Students may only use cell phones, smart phones, or other handheld or wearable devices with staff permission in accordance with to each building's policy.
B. Violation of building policies regarding cell phones, smart phones, or other handheld or wearable devices will be subject to the discipline policies of the school building.

5. PERIPHERAL DEVICES

A. Students will use peripherals under the direction and/or permission of staff members.
B. Users should print only when necessary and in quantities necessary.
C. Color printers may be used at the appropriate staff member's discretion.

UNACCEPTABLE USES OF TECHNOLOGY

The District strictly prohibits inappropriate uses of the Internet and District Network Resources, including email, web postings, text messages, and other online communications, which include but are not limited to the following:

A. Disclosure of confidential or sensitive information known or entrusted to the District to any unauthorized individual.
B. Misuse of copyrighted material or other copyright violations.
C. Communicating information that could be perceived as an official District position or endorsement without prior approval by proper District officials.
D. Using confrontational or improper language or making defamatory statements.
E. Creating, storing, viewing, or transmitting defamatory, pornographic, obscene, profane, illegal, or otherwise offensive material. If a user encounters such prohibited material, the user should immediately terminate contact with the material and notify appropriate District personnel.

F. Participating in any activity that could be interpreted as bullying, harassment, or discrimination.
G. Misrepresenting an individual's identity or the source of communications or data.
H. Attempting to break into any server, network, file, or similar activities.
I. Accessing confidential information via the District's network or District-provided cloud services without authorization.
J. Staff should not use district technology resources to promote political or religious positions (including violations of ethics and campaign disclosure laws).
K. Participating or engaging in activities that violate any local, state, federal, or international law, or any District policy, rule or standard.
L. Operating a personal business or using District network or technology resources for personal financial gain.
M. Disrupting the use of the District's network by other users, as in the case of a Denial of Service attack or preventing access to another user's files.
N. Distribution of spam emails.
O. Vandalizing District network or technology resources through any malicious act or the attempt to harm, modify, or destroy the computer property or data of the District or another user, the Internet, or District Network Resources, or any other technologies or devices used in the District. This includes but is not limited to causing physical damage to devices as well as participation in hacking or the uploading or creation of viruses or other malicious programs to any District network or technology resource.

HARASSMENT AND BULLYING

In accordance with Iowa law, the District's policy prohibiting bullying and harassment applies to all electronic communications. Employees and students are prohibited from engaging in any bullying or harassing behavior via any electronic means, including those means that are not part of the District's network and technology resources.

VIOLATIONS AND SANCTIONS

All users are expected to abide by the provisions of this Policy. Any student who uses technology in an unacceptable manner is in violation of the district's Student Behavior and Discipline Policy and will be subject to sanctions as stated in the policy. Since the nature of each violation may vary, the supervising classroom teacher and/or building administration is given broad discretion in determining the severity of the sanction, in accordance with any applicable building and district policies.

Staff members who use technology in an unacceptable manner may also be subject to disciplinary actions up to and including dismissal.

Violations of this Policy may also result in the loss of a user's privileges to use any or all District network or technology resources for an appropriate period of time to be determined by a building or District administrator. Sufficiently severe violations may result in permanent loss of privileges, as determined by a District administrator.

District staff or administration may confiscate any District-owned device from a student or employee, due to violation of this policy.

Reliability

The District makes no warranties of any kind, whether express or implied, for the service it is providing. The District will not be responsible for any damages that employees or other persons may suffer. This includes damages due to loss of data resulting from delays, failed message deliveries, equipment malfunctions, or service interruptions, whether caused by the District's own negligence or the employee's errors or omissions. The District specifically denies any responsibility for the accuracy or quality of information obtained through its services.

The ICCSD reserves the right to change this policy at any time. Students, parents and/or guardians will receive notification of any changes.

In compliance with federal law, this policy shall be maintained for at least five (5) years beyond the termination of funding under the Children's Internet Protection Act (CIPA) or E-Rate.