This administrative rule governs the use of the District's computer, internet and electronic research and communication resources and is intended to protect the integrity of District operations and instructional programs, as well as to outline the rights and responsibilities of District employees and students.

Scope

This administrative rule applies to the following persons/entities:

• All District employees including regular, part-time, temporary and contract employees

• All students enrolled in District schools

• All other authorized users of any of the District's technology resources, regardless of District affiliation or reason for usage

• All District owned or operated technology resources or systems which are subscribed to and/or paid for by the District

The personal life of an employee, including the employee's personal use of non-District issued electronic equipment outside of work hours (such as through social networking sites and personal portrayal on the Internet), will be the concern of and warrant the attention of the District if the employee's conduct impairs his/her ability to effectively perform his/her job responsibilities; if it results in a disruption of the school environment, or if the conduct violates Federal law, State law, and/or Board policy. Such conduct may subject the employee to disciplinary action, up to and including termination.

Staff Conduct

All employees shall maintain professional and appropriate relationships with students at all times, both inside and outside of school. No employee may engage in inappropriate or unprofessional conduct communicated or performed in person, in writing, or electronically through such means as a telephone, cell phone, computer, personal data assistant, or other telecommunication device, including text messaging, instant messaging and social networking.

Confidential Information

The District's research and communication resource systems have security measures in place; however, such measures do not guarantee total security. As a result, information generally considered to be personal or confidential, including personal information regarding students, should not be sent via the District's communication resources. The District prohibits the

unauthorized disclosure, use, and dissemination of personal information regarding minors via its electronic network. However, the District cannot assume responsibility for lost or stolen information sent or received via the District's communication resources.

General Computer Usage

The following actions are prohibited:

• Knowingly loading or creating viruses

• Loading or attempting to load software or files onto a school computer without the permission of the school's media specialist

• Loading or attempting to load software or files onto the District network without the permission of the Information Technology Department

• Accessing or modifying data without authorization

• Modifying passwords without authorization

• Computer vandalism, defined as any malicious or unauthorized attempt to harm or destroy equipment or data, files, or other electronic information not belonging specifically to the user

Internet Usage

Access to the Internet is made available to authorized users for educational and District operational purposes. All authorized users will receive instruction on proper use of the District's internet system. The District will educate minors about appropriate online behavior, including interacting with other individuals on social networking websites, in chat rooms, and with e-mail and other direct electronic communications, as well as cyberbullying awareness and response.

The District prohibits the use of its Internet system to intentionally access, view, download, store, transmit, or receive any information that contains material which is in violation of any District policy or administrative rule, or any local, state and/or federal laws or regulations. Prohibited material includes, but is not limited to:

• Obscenity or pornography

• Threats

• Material that is intended, or could reasonably be perceived, to be harassing or discriminatory

• Material that is copyrighted or protected by trade secret

• Material used to further any commercial business, product advertising, virus transmission or political activity

• Material that is potentially disruptive to the learning environment.

• For student use, materials that are inappropriate for or harmful to minors

In compliance with the Children's Internet Protection Act (CIPA), 47 U.S.C. § 254(h), the District utilizes technology protection measures to block and/or filter Internet access to images that are obscene, depict child pornography, and, for computers utilized by students, are otherwise harmful to minors. In addition, the District will monitor the online activities of minors, as appropriate, when utilizing District computers and Internet system. However, the District recognizes that it is impossible to control access to all inappropriate or controversial materials and prevent all unauthorized activities of users. Therefore, the District will take the appropriate disciplinary action against students and personnel for unauthorized access, including so-called "hacking," other unlawful activities utilizing the District internet system, and violations of this policy.

The Internet can provide a vast collection of educational resources for students. It is a global network that makes it impossible to control all available information. Because information appears, disappears and changes constantly, it is not possible to predict or control what students may locate. The school district makes no guarantees as to the accuracy of information received on the Internet. Although students will be under teacher supervision while on the network, it is not possible to constantly monitor individual students and what they are accessing on the network. Some students might encounter information that is not of educational value.

The District reserves the right to monitor and/or review all uses of the District Internet system and users should not have any expectation of privacy in any information accessed, viewed, downloaded, stored, transmitted, or received on the District's Internet system.

Rules Governing Use

All District digital and online content must comply with district policies on FERPA, data privacy, and public use of school records.

The District will not be responsible for any obligations resulting from any unauthorized use of the system. This includes, but is not limited to, copyrighted material, threatening or obscene material, material protected by trade secret, inappropriate materials of any kind, unauthorized

commitments to purchase items or services, purchase of software, upgrades to programs, or any illegal act.

The District will involve law enforcement should illegal activities take place.

Accessing inappropriate sites

Student Internet activities will be monitored by the district to prevent students from accessing inappropriate sites that have visual depictions that include obscenity, child pornography or are harmful to minors. The District will use technology protection measures to protect students from inappropriate access.

The District expects users to immediately report if they mistakenly access inappropriate information or images, any message they receive that they feel is inappropriate or that makes them feel uncomfortable, and any possible security problems. By immediately reporting, users protect themselves against allegations that they have intentionally violated the technology acceptable use policy. Students will immediately tell their attending teacher. Employees will immediately notify their supervisor.

Students will not post personal contact information about themselves or others unless it is in conjunction with a specific teacher-approved assignment or approved college/career communication. Personal contact information includes, but is not limited to, home address, telephone numbers, school address, etc.

Users will not attempt to gain unauthorized access to the email system, the district's digital and online content, or any other computer systems through the District's email, Internet, or network access.

Users will not use defamatory, false, obscene, profane, lewd, vulgar, rude, inflammatory, threatening, bullying, disrespectful, disruptive, racial, violent, or any other inappropriate language in public messages, private messages, and any material posted on digital and online content. All communications via district digital and online content will comply with the district's technology policy and district's student code of conduct policy and administrative rule.

Reporting

District and school computer technicians as well as other district employees who are working with a computer and come across sexually explicit images of children must report this to local law enforcement. The report must include the name and address of the owner or person in possession of the computer.

Plagiarism and Copyright

Users will not plagiarize works that they find on the Internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were original to the user. Users will use proper bibliography formats.

Users will respect copyright laws. Copyright infringement occurs when an individual inappropriately reproduces a work that is protected by copyright. If a work contains language that specifies acceptable use of that work, users should request permission from the owner.

Off-campus conduct

Students, parents/legal guardians, teachers and staff members should be aware that the district may take disciplinary actions for conduct initiated and/or created off-campus involving the inappropriate use of the Internet or web-based resources if such conduct poses a threat or substantially interferes with or disrupts the work and discipline of the schools, including discipline for student harassment and bullying, regardless of whether the action involved district or personal equipment or the source of access.

Electronic Mail (Email) Usage

The District's email system is made available to authorized users for educational and District operational purposes. All authorized users will receive instruction on proper use of the District email system. The District will assign email addresses to users. Student emails will associate with their Student Login numbers already assigned. All users will utilize the email appropriately and according to policy, regulations and guidelines. The email address can be utilized to access the District sponsored programs such as Office 365, One Note, etc.

The District prohibits the use of its email system for unprofessional and/or inappropriate purposes, to include, but not be limited to:

• Creating, transmitting or receiving emails containing any language or depictions that could reasonably be perceived by others as being offensive, threatening, obscene, sexual or racist

• Any use that violates local, state and/or federal laws or regulations

• Setting up or operating a commercial business

• Parents have the right to monitor all email correspondence of their child with username and password

• The only person who should use an account is the person to whom it is assigned (unless otherwise specified in an IEP or 504 Plan). Family members should not use the account.

• After a student graduates, the email account will be suspended after three months to allow correspondence with colleges, etc. If a student leaves the District, their account will be suspended immediately unless requested in writing through the school principal.

• All electronic messages created, transmitted or received via the District's email system, including those created, transmitted or received for personal use, are the property of the District. The District reserves the right to monitor and/or review all use of its email system and users should not have any expectation of privacy in any electronic message created, transmitted or received on the District's email system.

Handheld Communication Device Usage

District-issued cell phones or other handheld communication devices are to be used only by the employee to whom the phone or communication device was issued and are to be used only for matters directly related to the employee's job responsibilities. The District reserves the right to monitor and/or review all use of District-issued phones and communication devices and users should not have any expectation of privacy in any use of a District-issued phone or communication device. Limited use of cell phones and/or handheld devices in the classroom is permitted at the discretion of the classroom teacher.

Personal Use of District Research and Communication Resources

Limited personal use of District computer, Internet and electronic research and communication resources is permitted to the extent that such use does not disrupt or interfere with the operation of the District and its instructional programs. Excessive personal use that may or does so disrupt or interfere is prohibited.

Violations

All authorized users of District research and communication resources are expected to report any use that is believed to be unauthorized, excessive or otherwise in violation of this administrative rule. District employees who witness, experience, or otherwise learn about a suspected violation should report the matter to their immediate supervisor. Students who witness, experience or otherwise learn about a suspected violation should report the matter to a school administrator. Other authorized users who witness, experience, or otherwise learn about a suspected violation should report the matter to a District administrator.

All suspected violations will be investigated thoroughly. If it is determined that a violation of this administrative rule has occurred, the following disciplinary and/or corrective actions may be taken:

• Review of and possible changes to the level of supervision and the circumstances under which use is allowed

• Limitation, suspension and/or termination of the violator's use privileges

• For student violators, disciplinary measures consistent with the District's student discipline code, up to and including expulsion

• For employee violators, disciplinary measures determined to be appropriate based on the seriousness of the violation, up to and including termination

• Report to law enforcement when the violation is believed to constitute a violation of a Federal or State law or regulation and/or Board policy.