School District of Clay County

Student Responsible Use Guidelines for Technology

(Terms and Conditions for Use of Telecommunications and Networks - Reference School Board Policy 4.59)

The School District of Clay County makes a variety of communications and information technologies available to students through computer/network/Internet access. These technologies, when properly used, promote educational excellence in the District by facilitating resource sharing, innovation, and communication. Illegal, unethical or inappropriate use of these technologies can have devastating consequences, harming the District, its students and its employees. These Responsible Use Guidelines are intended to minimize the likelihood of such harm by educating District students and setting standards of use which will serve to protect the District. The District firmly believes that the advantages of having digital resources, information and interaction available on the computer/network/Internet far outweigh any disadvantages.

Mandatory Review. To educate students on proper computer/network/Internet use and conduct, students are required to review these guidelines at the beginning of each school year. All District students shall be required to acknowledge receipt and understanding of all guidelines governing use of the system and shall agree in writing to comply with said guidelines and to allow monitoring of their use of computers and other technology. The parent or legal guardian of a student user is required to acknowledge receipt and understanding of the District's Student Responsible Use Guidelines for Technology (hereinafter referred to as the Responsible Use Guidelines) as part of their review of the *Student Code of Conduct* handbook. Employees supervising students who use the District's computer/network/internet system must provide training emphasizing its appropriate use.

Definition of District Technology System. The District's computer systems and enterprise network are any configuration or combination of hardware and software. The system includes but is not limited to the following:

- Telephones, cellular telephones, and voicemail technologies;
- Email accounts;
- Servers;
- Computer hardware and peripherals;
- Software including operating system software and application software;
- Digitized information including stored text, data files, email, digital images, and video and audio files;
- Internally or externally accessed databases, applications, or tools (Internet- or District-server based);
- District-provided Internet access;
- District-filtered Wi-Fi; and
- New technologies as they become available.

Availability of Access

Acceptable Use. Computer/Network/Internet access will be used to enhance learning consistent with the District's educational goals. The District requires legal, ethical and appropriate computer/network/Internet use.

Privilege. Access to the District's computer/network/Internet is a privilege, not a right.

Access to Computer/Network/Internet. Access to the District's electronic communications system, including the Internet, shall be made available to students for instructional purposes. Each District computer has filtering software that blocks access to visual depictions that are obscene, pornographic, inappropriate for students, or harmful to minors, as defined by the federal Children's Internet Protection Act (CIPA). Filtered Internet access is provided to students as defined by CIPA.

Student Access. Computer/Network/Internet access is provided to all students unless parents or guardians submit a written request to the campus principal that access be denied. Student Internet access will be under the direction and guidance of a District staff member. Students may also be allowed to use the local network and Wi-Fi with campus permission.

Students 13 or younger. For students under the age of 13, the Children's Online Privacy Protection Act (COPPA) requires additional parental permission for student access to educational software tools. Parents wishing to deny access to these educational tools must submit a request in writing to the campus principal directing that their child should be denied access to these tools. These tools are accessed by the student through the District's student Webpage.

Security. A student who gains access to any inappropriate or harmful material is expected to discontinue the access and to report the incident to the supervising staff member. Any student identified as a security risk or as having violated the Responsible Use Guidelines may be denied access to the District's system. Other consequences may also be assigned. A student who knowingly brings prohibited materials into the school's electronic environment shall be subject to suspension of access to, and/or revocation of privileges on, the District's system and shallbe subject to disciplinary action in accordance with the Board-approved *Student Code of Conduct*.

Content/Third-Party Supplied Information. Students and parents of students with access to the District's system should be aware that use of the system may provide access to other electronic communication systems in the global electronic network which may contain inaccurate and/or objectionable material.

Subject to Monitoring. District computer/network/Internet usage is not confidential and is subject to monitoring by designated staff at any time to ensure appropriate use. Students should not use the computer system to send, receive or store any information, including email messages, that they consider personal or confidential and wish to keep private. All electronic files, including email messages, transmitted through or stored in the computer system will be treated no differently than any other electronic file. The District reserves the right to access, review, copy, modify, delete or disclose such files for any purpose. Students should treat the computer system like a shared or common file system with the expectation that electronic files, sent, received or stored anywhere in the computer system, will be available for review by any authorized representative of the District for any purpose. Personal telecommunication devices used to connect with District computer/network/Internet systems are subject to examination in accordance with disciplinary guidelines if there is reason to believe that the Responsible Use Guidelines have been violated.

Student Computer/Network/Internet Responsibilities

District students are bound by all portions of the Responsible Use Guidelines. A student who knowingly violates any portion of the Responsible Use Guidelines shall be subject to suspension of access to, and/or revocation of privileges on, the District's system and shall be subject to disciplinary action in accordance with the Board-approved *Student Code of Conduct*.

Use of Social Networking/Digital Tools. Students may participate in District-approved social media learning environments related to curricular projects or school activities and use digital tools, including, but not limited to, mobile devices, blogs, discussion forums, RSS feeds, podcasts, wikis, and on-line meeting sessions as directed by a teacher or staff member. The use of blogs, wikis, podcasts, and other digital tools are considered an extension of the classroom. Verbal or written language that is considered inappropriate in the classroom is also inappropriate in all uses of blogs, wikis, podcasts, and other District-approved digital tools.

Use of System Resources. Students are directed to purge email or outdated files on a regular basis.

Password Confidentiality. Students are required to maintain password confidentiality by not sharing their password with others. A student may not use any another person's system account.

Reporting Security Problem. If knowledge of inappropriate material or a security problem on the computer/network/Internet is identified, the student shall immediately notify the supervising staff member. The inappropriate material/security problem shall not be shared with others.

Inappropriate Use

Inappropriate use of the District computer/network/internet system includes, but is not limited to, those uses that violate federal and state law, that are specifically named as violations in this document, that violate the rules of network etiquette, or that hamper the integrity or security of this computer/network/Internet system or any components that are connected to it. The following actions are considered inappropriate uses, are prohibited, and will result in suspension of access to, and revocation of the student's privileges on, the District's computer/network/Internet system.

- threatening, harassing, defamatory or obscene material;
- unauthorized use of copyrighted material;
- use of plagiarized material;
- unauthorized use of material protected by trade secret; or
- accessing blog posts, Web posts, or discussion forum/replies posted to the Internet which violate federal or state law.

Tampering with or theft of components from District systems may be regarded as criminal activity under applicable state and federal laws. Any attempt to break the law through the use of a District computer/network/Internet account may result in prosecution against the offender by the proper authorities. If such an event should occur, the District will fully comply with the authorities to provide any information necessary for legal action.

Modification of Computer. Modifying or changing computer settings and/or internal or external configurations without District permission is prohibited.

Transmitting Confidential Information. Students may not redistribute or forward confidential information about themselves or any other student without District authorization. Confidential information should never be transmitted, redistributed or forwarded to individuals outside the District who are not expressly authorized by District personnel to receive the information. Revealing personal information about oneself or others, including, but not limited to, home addresses, phone numbers, email addresses, birthdates is prohibited.

Commercial Use. Use of the system for any type of income-generating activity is prohibited. Advertising the sale of products, whether commercial or personal is prohibited.

Marketing by Non-SDCC Organizations. Use of the system for promoting activities or events for individuals or organizations not directly affiliated with or sanctioned by the District is prohibited.

Vandalism/Mischief. Any malicious attempt to harm or destroy District equipment, materials or data; or the malicious attempt to harm or destroy data of another user of the District's system, or any of the agencies or other networks to which the District has access is prohibited. Deliberate attempts to degrade or disrupt system performance are violations of District policy and administrative regulations and may constitute criminal activity under applicable state and federal laws. Such prohibited activity includes, but is not limited to, the uploading or creating of computer viruses.

Vandalism as defined above is prohibited and will result in the cancellation of system use privileges. Students committing vandalism will be required to provide restitution for costs associated with system restoration and may be subject to other appropriate consequences as provided for in the Board-approved *Student Code of Conduct*.

Intellectual Property. Students shall, at all times, respect copyrights and trademarks of third-parties and their ownership claims in images, text, video and audio material, software, information and inventions. The copying, use, or transfer of others' materials without appropriate authorization prohibited.

Copyright Violations. Downloading or using copyrighted information without following approved District procedures is prohibited.

Plagiarism. Fraudulently altering or copying documents or files authored by another individual is prohibited.

Impersonation. Attempts to log on to the computer/network/Internet impersonating a system administrator or District employee, student, or individual other than oneself, will result in revocation of the student's access to computer/network/Internet.

Illegally Accessing or Hacking Violations. Intentional or unauthorized access or attempted access of any portion of the District's computer systems, networks, or private databases to view, obtain, manipulate, or transmit information, programs, or codes is prohibited.

File/Data Violations. Deleting, examining, copying, or modifying files and/or data belonging to other users, without their permission is prohibited.

System Interference/Alteration. Deliberate attempts to exceed, evade or change resource quotas are prohibited. Deliberately causing network congestion through mass consumption of system resources is prohibited.

Email and Communication Tools

Email and other digital tools including, but not limited to blogs and wikis, are tools used to communicate within the District. The use of these communication tools shall be limited to instructional, school-related activities, or administrative needs.

All students in grades 6-12 will be issued email accounts. Students should check email frequently, delete unwanted messages promptly, and stay within the email server space allocations. Email attachments are limited to 20MB or smaller. Internet access to personal email accounts is prohibited.

Students should keep the following points in mind:

Perceived Representation. Using school-related email addresses, blogs, wikis, and other communication tools might cause some recipients or other readers of the email to assume that the student's comments represent the District or school, whether or not that was the student's intention.

Privacy. Email, blogs, wikis, and other communication within these tools are not considered a private, personal form of communication. Private information, such as home addresses, phone numbers, last names, pictures, or email addresses, shall not be divulged. To avoid disclosing email addresses that are protected, all email communications to multiple recipients shall be sent using the blind carbon copy (bcc) feature.

Inappropriate Language. Using obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language in emails, blogs, wikis, or other communication tools is prohibited. Sending messages~~,~~ that could cause danger or disruption, including personal attacks~~,~~and prejudicial or discriminatory attacks, is prohibited.

Political Lobbying. Consistent with State ethics laws, District resources and equipment, including, but not limited to, emails, blogs, wikis, or other communication tools shall not be used to conduct any political activity, including political advertising or lobbying. This prohibition includes using District email, blogs, wikis, or other communication tools to create, distribute, forward, or reply to messages, from either internal or external sources, which expressly or implicitly support or oppose a candidate for nomination or election to either a public office or an office of a political party or which support or oppose an officeholder, a political party, or a measure (a ballot proposition). These guidelines prohibit direct communications as well as the transmission or forwarding of emails, hyperlinks, or other external references within emails, blogs, or wikis regarding any political advertising or other political or lobbying activity prohibited by this paragraph.

Forgery. Forgery or attempted forgery of email messages is prohibited. Attempts to read, delete, copy or modify the email of other system users, deliberate interference with the ability of other system users to send/receive email, or the use of another person's user ID and/or password is prohibited.

Junk Mail/Chain Letters. Students shall refrain from forwarding emails which do not relate to the educational purposes of the District. Chain letters or other similar emails intended for forwarding or distributing to others are prohibited. Creating, distributing or forwarding any annoying or unnecessary message to a large number of people (spamming) is prohibited.

Student Email Accounts and Electronic Communication Tools

Electronic communication is an important skill for 21st Century students. By providing this tool, the District is equipping students with the skills necessary for success in the business. Students in grades 6 - 12 are given access to a District student email account. This account is set up with the student's user ID. Students must abide by the guidelines established at Email and Communication Tools. Student email accounts will be available for use by students in grades 6-12 while they are currently enrolled in the District. Parents wishing to deny access to District email must submit a request for such denial in writing to the campus principal. Project email accounts may be granted for educational activities for students in grades K-5 as deemed appropriate by, and at the request of, the District Administration. Student email accounts may be provided directly by the District, through the content management system of an approved online course, or through a District-approved provider.

Consequences of Agreement Violation

Any attempt to violate the provisions of this agreement may result in revocation of the student's access to the computer/network/Internet, regardless of the success or failure of the attempt. In addition, school disciplinary and/or appropriate legal action may be taken.

Denial, Revocation, or Suspension of Access Privileges. With just cause, the System Administrator and/or building principal, may deny, revoke, or suspend computer/network/Internet access as required, pending an investigation.

Failure to Adhere to Academic Integrity of Online Courses. Florida Statue 1002.321(5) states: It is unlawful for any person to knowingly and willfully take an online course or examination on behalf of another person for compensation. Any person who violates this subsection commits a misdemeanor of the second degree, punishable as provided in s. 775.082 or s. 775.083.

Warning

Sites accessible via the computer/network/Internet may contain material that is illegal, defamatory, inaccurate or controversial. Each District computer with Internet access has filtering software that blocks access to visual depictions that are obscene, pornographic, inappropriate for students, or harmful to minors, as defined by the federal Children's Internet Protection Act. The District makes every effort to limit access to objectionable material; however, controlling all such materials on the computer/network/Internet is impossible, even with filtering in place. With global access to computers and people, a risk exists that students may access material that may not be of educational value in the school setting.

Disclaimer

The District's system is 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 guarantee 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 system are those of the providers 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.