STUDENT ACCEPTABLE USE AND INTERNET SAFETY POLICY

Code **IJNDB** *Issued* **6/17**

Purpose: To establish the board's vision and the basic structure for acceptable use of technology resources, the Internet and the technology network system by students in the Sumter School District.

Sumter School District will provide for the education of minors about inappropriate online behavior including interacting with other individuals on social networking sites and in chat rooms, and cyberbullying awareness and response.

Acceptable Use

The Internet and technology network system in the Sumter School District has been established for a limited educational purpose. The term "educational purpose" includes the following.

- classroom activities
- career development
- limited, high-quality, independent student activities

The technology network system has not been established as a public access service or a public forum. The district has the right to place reasonable restrictions on the materials students access or post through the system. Students are also expected to follow the rules set forth in the Acceptable Use Policy (AUP), the district's disciplinary code and the law in their use of the district's network system.

This policy applies to computers installed in the school, district laptops provided to students either temporarily or permanently, and any personal equipment brought onto campus capable of Internet access.

Students may not use the district network system for commercial purposes. This means that students may not offer, provide or purchase products or services through the system.

Students may not use the district network system for lobbying. Students may use the system to communicate with elected representatives to express opinions on political issues under the guidance of instructional personnel.

Privileges

The use of the Internet is a privilege, not a right. Inappropriate use will result in a cancellation of that privilege and possible disciplinary action. Each student licensed to access the Internet on district-owned computers or district laptops provided to students will receive training from a staff member on appropriate general Internet policy and, where appropriate, will receive additional specific guidance on projects or work being assigned. In circumstances not covered by the general guidance outlined in this agreement, the staff will deem what is inappropriate use and their decisions are final. District laptops provided to students should not be used in the gym, at lunch or in the hallways. Use in the classroom is at the sole discretion of the teacher. Use of the computer on campus for entertainment purposes (watching DVD movies, listening to MP3 music, playing games, etc.) is prohibited.

(see next page)

PAGE 2 - IJNDB - STUDENT ACCEPTABLE USE AND INTERNET SAFETY POLICY

Student Internet Access

All students will have access to online digital information resources through their classroom, library or school computer lab. Parents/Legal guardians must sign and return an Internet access agreement (IJNDB-E) prior to individual student's use of the Internet until the student's 18th birthday. Only those students with signed AUPs may sit next to other students accessing the Internet.

Secondary students may obtain an individual e-mail account with the approval of their parents/legal guardians until age 18.

Students and their parents/legal guardians must sign an account agreement to be granted an individual e-mail account. This agreement must be renewed on an annual basis. Parents/legal guardians can withdraw their approval at any time, until the student's 18th birthday.

If approved by their building principal, students may create a personal web page on the district's network system. All material placed on their web page must be preapproved in a manner specified by the school. Material placed on their web pages must relate to the school and career preparation activities.

Unacceptable Uses

The following uses of the district's network systems are considered unacceptable.

Personal safety

Students will not post personal contact information about themselves or other people. Personal contact information includes home addresses, telephone numbers, work addresses, etc.

Students will agree not to meet with someone they corresponded with online without their parents/legal guardians' approval.

Students will promptly disclose to their teacher or other school employee any message they receive that is inappropriate or makes them feel uncomfortable.

Illegal activities

Students will not attempt to gain unauthorized access to the district's network system or to any other computer system through the district or go beyond their authorized access. This includes attempting to log in through another person's account or to access another person's files.

Students will not make deliberate attempts to disrupt the computer system or destroy data by spreading computer viruses or by any other means. These actions are illegal.

Students will not use the district network system to engage in any other illegal act, such as arranging for a drug sale or purchasing of alcohol, engaging in criminal gang activity, threatening the safety of a person, etc.

Students will not participate in chats, instant messaging services or social networking, or play computer games on school computers unless authorized by a district staff member for legitimate educational purposes.

Students will not make changes to or tamper with the setting on computers, CD-ROMS or any attached equipment on the network.

(see next page)

Vandalism

Vandalism is defined as any malicious attempt to harm or destroy hardware or the data of another user or other network (school, Internet or Google Apps for Education account). The intentional uploading, distribution or creation of computer viruses is also considered acts of vandalism. Vandalism will result in immediate cancellation of all computer privileges. Discipline will be assessed in accordance with the current grade-level discipline code. Students will be responsible for payment of any damages to any hardware or software.

System security

Students are responsible for their individual account and should take all reasonable precautions to prevent others from being able to use their account. Under no conditions should students provide their password to another person.

Students will immediately notify a teacher or the system administrator if they have identified a possible security problem.

Students will not set or reset passwords without approval from district staff.

Students will avoid the inadvertent spread of computer viruses by following the district virus protection procedures. Any removable media (thumb/flash drives, CD-R/RWs, etc.) brought from outside the school must be checked by a district staff member for viruses prior to use in district computers and/or laptops.

Inappropriate language

Restrictions against inappropriate language apply to public messages, private messages and material posted on web pages.

Students will not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening or disrespectful language.

Students will not engage in personal attacks, including prejudicial or discriminatory attacks.

Students will not harass or cyberbully another person. Harassment is defined as persistently acting in a manner that distresses or annoys another person. If a student is told by a person to stop sending messages, the student must stop.

Students will not knowingly or recklessly post false or defamatory information about a person or organization that could cause damage or pose a danger of disruption.

Respecting resource limits

Students will use the system only for educational and career development activities and limited, high-quality, independent student activities. There is no limit on use for education and career development activities. The limit on activities is no more than five hours per week. Students will strictly observe time limits.

Students will not download large files unless absolutely necessary and approved by a district staff member. If necessary, students will download the file at a time when the system is not being heavily used and immediately remove the file from the system computer to a personal computer.

(see next page)

PAGE 4 - IJNDB - STUDENT ACCEPTABLE USE AND INTERNET SAFETY POLICY

Students will obtain permission from a staff member before printing pages.
Students will not post chain letters or engage in "spamming." Spamming is defined as sending an annoying or unnecessary message to a large number of people.

Students will check their e-mail frequently, delete unwanted messages promptly and stay within their e-mail quota.

Students will subscribe only to high quality discussion group mail lists that are relevant to their education or career development.

While on campus, students will not use private e-mail. Students at schools use Google Apps for Education G Suite for email, electronic filing and class pages in accordance with published guidelines provided the following is adhered to.

- Parents/legal guardians have approved such access on the appropriate form (IJNDB-E).
- Students have completed CIPA Compliance training at their school.
- Students successfully have signed on with Google Apps for Education to access G Suite.

Plagiarism and copyright infringement

Students will not plagiarize works found on the Internet. Plagiarism is defined as taking the ideas or writings of others and presenting them as if they were the writer's.

Students will respect the rights of copyright owners. Copyright infringement occurs when a student inappropriately reproduces a work that is protected by a copyright. If a work contains language that specifies appropriate use of that work, students should follow the expressed requirements. If students are unsure whether or not they can use a work, they should request permission from the copyright owner. Proper citation for all work used is required.

Reporting

District and school system technicians 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.

Inappropriate access to material

Students will not use the district's network system to access material that is profane or obscene (pornography or child pornography), that advocates illegal acts or that advocates violence or discrimination towards other people (hate literature). If a student mistakenly accesses inappropriate information, he/she should immediately tell the teacher or another district employee. This will protect students against a claim that they have intentionally violated this policy.

Students' parents/legal guardians should inform district staff if there is additional material that they think would be inappropriate for their children to access. The district fully expects that students will follow their parents/legal guardians' instructions in this matter.

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

(see next page)

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.

Student Rights

Free speech

Students' right to free speech, as set forth in the disciplinary code, applies also to their communication on the Internet. The district network system is considered a forum, similar to the school newspaper; therefore, the district may restrict student speech for valid educational reasons. The district will not restrict student speech on the basis of a disagreement with the opinions.

Search and seizure

Students should expect only limited privacy in the contents of their personal files on the district system. This situation is similar to the rights students have in the privacy of their lockers.

Routine maintenance and monitoring of the district network system may lead to discovery that the students have violated this policy, the disciplinary code or the law.

An individual search will be conducted if there is reasonable suspicion that a student has violated this policy, the disciplinary code or the law. The investigation will be reasonable and related to the suspected violation.

Parents/legal guardians have the right at any time to request to see the contents of their child's e-mail files, until the student's 18th birthday.

Due process

The district will cooperate fully with local, state and federal officials in any investigation related to any illegal activities conducted through the district's network system.

In the event there is a claim that a student violated this policy or disciplinary code in their use of the district network system, the student will be provided with a written notice of the suspected violation and given the opportunity to present an explanation before an administrator. If the violation also involves a violation of other provisions of the disciplinary code, it will be handled in a manner described in the disciplinary code. Additional restrictions may be placed on the student's use of an Internet account.

Limitation of Liability

The Internet can provide a vast collection of educational resources for students and employees. 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 makes no guarantee that the functions or the services provided by or through the district system will be error-free or without defect. The district will not be responsible for any

damage students may suffer including, but not limited to, loss of data or interruptions of service. The district is not responsible for the accuracy or quality of the information obtained through or stored on the system. The district will not be responsible for financial obligations arising through the unauthorized use of the system.

Adopted 6/13/11; Revised 11/26/12, 6/5/17

Legal References:

A. Federal law:
   1. 47 USC Section 254(h) - Children's Internet Protection Act.
   2. The Digital Millennium Copyright Act of 1998, Section 512 - Limitations on liability relating to material online.

B. S.C. Code of Laws, 1976, as amended:
   1. Section 10-1-205 - Computers in public libraries; regulation of Internet access.
   2. Section 16-3-850 - Encountering child pornography while processing film or working on a computer.
   3. Section 16-15-305 - Disseminating, procuring or promoting obscenity unlawful; definitions; penalties; obscene material designated contraband.
   4. Section 59-19-90 - General powers and duties of school trustees.

C. Court cases:
   1. *Purdham v. Fairfax Co. Sch. Bd.*, 637 F.3d 421, 427 (4th Cir. 2011).