Appropriate Use Policy of Sumter County Schools Computers and Network Resources

It is the belief of the Sumter County Board of Education that the use of technology for the purpose of information acquisition and retrieval is an important part of preparing children to live in the 21st century. The Board further believes that a "technology rich" classroom can significantly enhance both the teaching and learning process. This technology includes computer hardware, software, local and wide area networks and access to the Internet. Due to the complex nature of these systems and the magnitude of information available via the Internet, the Sumter County Board of Education believes guidelines regarding acceptable use are warranted in order to serve the educational needs of students.

It shall be the policy of the Sumter County Board of Education that the school system shall have in continuous operation, with respect to any computers belonging to the school having access to the Internet:

1. A qualifying "technology protection measure," as that term is defined in Section 1703(b)(1) of the Children's Internet Protection Act of 2000; and
2. Procedures or guidelines developed by the superintendent, administrators and/or other appropriate personnel which provide for monitoring the online activities of users and the use of the chosen technology protection measure to protect against access through such computers to visual depictions that are (i) obscene, (ii) child pornography, or (iii) harmful to minors, as those terms are defined in Section 1703(b)(1) and (2) of the Children's Internet Protection Act of 2000. Such procedures or guidelines shall be designed to:
    a. Provide for monitoring the online activities of users to prevent, to the extent practicable, access by minors to inappropriate matter on the Internet and the World Wide Web;
    b. Promote the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications;
    c. Prevent unauthorized access, including so-called "hacking," and other unauthorized activities by minors online;
    d. Prevent the unauthorized disclosure, use and dissemination of personal identification information regarding minors; and
    e. Restrict minors' access to materials "harmful to minors," as that term is defined in Section 1703(b)(2) of the Children's Internet Protection Act of 2000.

The district's technology resources are provided for educational purposes that promote and are consistent with the instructional goals of the Sumter County School System. Use of computers and network resources outside the scope of this educational purpose is strictly prohibited. Students and employees accessing network services or any school computer shall comply with the district's acceptable use guidelines. The district reserves the right to monitor, access, and disclose the contents of any user's files, activities, or communications. Email accounts are provided to teachers and students as long as they are active in the school system. They will be deleted when their status changes.

It must also be understood that the Internet is a global, fluid community, which remains largely unregulated. While it is an extremely valuable tool for educational research, there are sections that are not commensurate with community, school, or family standards. It is the belief of the Board that the Internet's advantages far outweigh its disadvantages. The Sumter County Board of Education will, through its administrative staff, provide an Internet screening system which blocks access to a large percentage of inappropriate sites. It should not be assumed, however, that users are completely prevented from accessing inappropriate materials or from sending or receiving objectionable communications.

Additionally, access to the Internet and computer resources is a privilege, not a right. Therefore, users violating the Sumter County Board of Education's acceptable use policy shall be subject to revocation of these privileges and potential disciplinary action.

Sumter County Schools Computers and Network Resources Employee Acceptable Use Guidelines

Please read the following carefully. Violations of the Acceptable Use Guidelines may cause an employee's access privileges to be revoked, School Board disciplinary action and/or appropriate legal action may be taken, up to and including employment termination.

Additional items that employees need to be aware of:

A. Staff must be aware that students have access to the Internet from all of the school system's computers. Teachers must use good judgment and closely supervise their student's use of the Internet. The School System uses filtering software to help prevent student access to inappropriate web sites. However, it is impossible to block access to all objectionable material. If a student decides to behave in an irresponsible manner, they may be able to access sites that contain materials that are inappropriate for children or are not commensurate with community standards of decency. They should not be permitted to access sites unrelated to their assignment and should not be allowed to access game or other sites that could infect the computer with “Spyware”.

B. Teachers should follow the guidelines below when allowing or directing students to do Internet searches.
   Elementary:
   Students in grades K-5 may visit sites pre-selected by a teacher. Searches may only be done with child-friendly Internet search engines **and** must be done with teacher supervision.
   Middle:
   Students in grades 6-8 may only perform unsupervised Internet searches using child-friendly search engines. A search using any other search engine must be conducted with teacher supervision.
   High:
   If students in grades 9-12 use any search engines other than a child-friendly search engine, they must use the advanced search page of internet search engines in order to develop more reliable, useful, and relevant search results.

C. Any individual who is issued a password is required to keep it private and is not permitted to share it with anyone for any reason.

D. Never allow a student to log in with a staff member's user name and password. They will tell their friends what the password is and they will log in under the teacher name and look at private documents including e-mail and grades.

E. Be careful when entering your user name and password or changing your password. Students will try to look over your shoulder and steal this information.

F. Enforce the Acceptable Use Guidelines while supervising students. For example, students should not have access to a command prompt or other software applications not accessible through the student menu. It is the employee's responsibility to notify the administration and the Technology Department of any violation of the Acceptable Use Policy.

G. Do not allow students to go to computer labs unsupervised (if the school site has labs).

H. Treat student user names and passwords with confidentiality. Do not post a list of user names and passwords where all students can see them.

I. Users are responsible for the appropriate storage and backup of their data.

J. The system requires employees to change passwords every 60 days. Some examples of passwords not to use: names of pets, birth date, children's names, street address, school mascots, favorite car, sports team, actor or movie. Do not record your login or password for your security.

K. Short-term substitute teachers are not to take students to the computer lab nor allow students to use the computers in the classrooms. (Long term substitute teachers may be qualified to use computers/labs after they receive appropriate orientation including review of the Acceptable Use Policy.)

L. Email accounts are provided to employees for professional purposes. Email accounts should not be used for personal gain or personal business activities; broadcasting of unsolicited messages is prohibited. Examples of such broadcasts include chain letters, mail bombs, virus hoaxes, SPAM mail (spreading email or postings without good purpose), religious notes, and executable files. These types of email often contain viruses and can cause excessive network traffic or computing load.
M. Employees are not permitted to connect or install any computer hardware, components, or software, which are not school system property to or in the district's technology resources without prior approval of the district technology supervisory personnel.
N. Employees are not permitted to use the school's computer hardware or network for any illegal activity such as copying or downloading copyrighted software, music or images, or violation of copyright laws.
O. Employees are not permitted to download, install, or use games, music files, public domain, shareware or any other unauthorized program on any school's computer or computer system.
P. Employees must abide by the Sumter County Schools Web Site Posting guidelines when posting any materials to the web.

Sumter County Schools Computers and Network Resources Student Acceptable Use Guidelines

Please read the following carefully. Violations of the Acceptable Use Guidelines may cause a student's access privileges to be revoked, disciplinary action and/or appropriate legal action may be taken.

Any student who utilizes the computer lab(s) or any computer equipment at the school must be aware of certain policies for use of the equipment and/or facilities. Procedures are in place for the protection of students and equipment. Students will be held accountable for any violation of the following policies (as would be the case for any classroom disciplinary matter). A student and his/her parents will be responsible for damages and will be liable for costs incurred for service or repair.

Students are only allowed to utilize the computers and network to retrieve information and run specific software applications as directed by their teacher. Students are not permitted to explore the configuration of the computer, operating system or network, run programs not on the menu, or attempt to do anything they are not specifically authorized to do.

Students are responsible for ensuring that any diskettes, CDs, memory sticks, USB flash drives, or other forms of storage media that they bring in from outside the school are virus free and do not contain any unauthorized or inappropriate files. Students may not bring personal computers or hand-held computing devices and connect them to the school network or Internet connection (including connecting to wireless access points).

Safety Issues:

1. Any on-line communication should always be at the direction and with the supervision of a teacher.
2. Never provide last name, address, telephone number, or school name online.
3. Never respond to, and always report to the teacher or parent, any messages that make you feel uncomfortable or that are from an unknown origin.
4. Never send a photo of yourself or anyone else.
5. Never arrange a face-to-face meeting with someone you met on-line.
6. Never open attachments or files from unknown senders.
7. Always report to a teacher any inappropriate sites that you observe being accessed by another user or that you browse to accidentally.

Examples of prohibited conduct include but are not limited to the following:

A. Accessing, sending, creating or posting materials or communications that are:
    1. Damaging to another person's reputation,
    2. Abusive,
    3. Obscene,
    4. Sexually oriented,
    5. Threatening or demeaning to another person,
    6. Contrary to the school's policy on harassment,
    7. Harassing, or
    8. Illegal
B. Using the network for financial gain or advertising.
C. Posting or plagiarizing work created by another person without their consent.
D. Posting anonymous or forging electronic mail messages.
E. Attempting to read, alter, delete, or copy the electronic mail messages of other system users.
F. Giving out personal information such as phone numbers, addresses, driver's license or social security numbers, bankcard or checking account information.
G. Using the school's computer hardware or network for any illegal activity such as copying or downloading copyrighted software, music or images, or violation of copyright laws.

H. Downloading, installing, or using games, music files, public domain, shareware or any other unauthorized program on any school's computer or computer system.
I. Purposely bringing on premises or infecting any school computer or network with a Virus, Trojan, or program designed to damage, alter, destroy or provide access to unauthorized data or information.
J. Gaining access or attempting to access unauthorized or restricted network resources or the data and documents of another person.
K. Using or attempting to use the password or account of another person or utilizing a computer while logged on under another user's account.
L. Using the school's computers or network while access privileges have been suspended.
M. Using the school's computer hardware, network, or Internet link in a manner that is inconsistent with a teacher's directions and generally accepted network etiquette.
N. Altering or attempting to alter the configuration of a computer, network electronics, the operating system, or any of the software.
O. Attempting to vandalize, disconnect or disassemble any network or computer component.
P. Utilizing the computers and network to retrieve information or run software applications not assigned by their teacher or inconsistent with school policy.
Q. Providing another student with user account information or passwords.
R. Connecting to or installing any computer hardware, components, or software which are not school system property to or in the district's technology resources without prior approval of the district technology supervisory personnel.
S. Bringing on premises any disk or storage device that contains a software application or utility that could be used to alter the configuration of the operating system or network equipment, scan or probe the network, or provide access to unauthorized areas or data.
T. Downloading or accessing via e-mail or file sharing, any software or programs not specifically authorized by Technology personnel.
U. Bypassing or attempting to circumvent network security, virus protection, network filtering, or policies.
V. Possessing or accessing information on school property related to “Hacking”, or altering, or bypassing network security or policies.
W. Participating on message boards without teacher direction, or in live chat using but not limited to AIM, Yahoo, or MSN Messenger.
X. Students should follow the guidelines below when performing Internet searches.

Elementary:
Students in grades K-5 may visit sites pre-selected by a teacher. Searches may only be done with child-friendly Internet search engines and must be done with teacher supervision.

Middle:
Students in grades 6-8 may only perform unsupervised Internet searches using child-friendly search engines. A search using any other search engine must be conducted with teacher supervision.

High:
If students in grades 9-12 use any search engines other than a child-friendly search engine, they must use the advanced search page of internet search engines in order to develop more reliable, useful, and relevant search results.

Sumter County Schools Computers and Network Resources Web Site Posting Guidelines

I. Student Information, Work, and Pictures:

1. Web pages hosted from Sumter County School District's web server may contain a reference to a student. This includes references to students in photographs or in text.
2. The following student information is acceptable to include in conjunction with text or photograph, unless parent(s) request that no information on their child be posted on the school's web page*.
    - A student's photograph or exemplary classroom projects may be posted, but the school system is careful not to associate a student's full name in such a way that it can be identified with a photograph of a student.

II. On Copyright

1. Unauthorized use of copyrighted material is prohibited. All copyrighted material must be properly cited using standard citation information. Giving credit (web address or active link) to a company or individual (celebrity, for instance) that has created text, a graphic, etc. for a school page may be allowed, assuming the site is not blocked by the web filtering hardware and software.

III. Prohibited Content/Items

1. Personal communications information about staff and parent volunteers: non-district email addresses, non-district mailing address, and non-district phone numbers except as approved by the building principal and the parent volunteer whose information is to be released.
   Example: PTSO/PTA/Booster Organization officer/contact requests to have their personal email address listed in the appropriate area on the school's page(s) and principal approves the request.
2. Student personal contact information of any kind
3. Links to staff, volunteers or student's "personal" home pages that are on remote, non-district web servers (not hosted on Sumter County School's equipment)
4. Links to "non-official" Sumter County Schools related sites that are hosted on remote, non-district web servers - Examples: athletic booster pages, PTA pages, etc. This prohibition includes teacher-created classroom pages or online services that may inform parents and visitors of the school district's site or classroom activities. The school system will provide hosting services for school-related web postings of booster club organizations, PTA groups, teachers, etc. following the same protocol and guidelines presented in this document.
5. Counters: If a school wants a Web page counter on its site, it must be an "invisible" counter. Tracking information on the use of a school's web site and individual sections can be obtained from Coordinator of Online Learning.

IV. Compliance with FCS Acceptable Use Guidelines

All material posted to the Sumter County Schools website must adhere to all provisions set forth in the Acceptable Use Guidelines. Items from these documents, which are relevant to information posted on the web, are:

No information/materials may be posted that is:

- Damaging to another person's reputation,
- Abusive,

- Obscene,
- Sexually oriented,
- Threatening or demeaning to another person's gender or race,
- Contrary to the school's policy on harassment
- Harassing
- Illegal

Pages created/information posted on Sumter County Schools web sites:

- MUST NOT use the network for financial gain or advertising.
- MUST NOT contain plagiarized work created by another person without his/her consent
- MUST NOT contain personal information such as phone numbers, addresses, drivers license or social security numbers, bank card or checking account information about any student or staff member.
- MUST NOT provide any user account information or passwords. If students participate in the creation and/or maintenance of web pages, they MUST be logged onto the network with their own USER IDs and PASSWORDS. Under NO circumstances are students to be given another student's or employee's login information.

V. Educational Appropriate Postings
Material posted to the school's web site and associated teacher web pages must be educationally sound and appropriate as determined by the school or district administrators.

* *Parent permission is granted in the Student Handbook.*

Sumter County Schools Email Disclaimer

Sumter County Schools has implemented a series of technology systems that “filter” all incoming email to detect SPAM (junk mail) and those that contain viruses, certain key words, html scripts, or have other attributes that could potentially be unacceptable for student viewing or compromise network security. Our system also uses a Bayesian filter that uses algorithms to identify messages that are probable SPAM. We have set the system to automatically redirect any email identified as SPAM to the junk mail folder.

We have had some emails sent to teachers, administrators and employees of the school system that have been reported as being blocked. We realize the scrutiny we get when email is tagged as SPAM, blocked and subsequently deleted. There are many reasons why an email may be blocked by our system and they have been listed at the bottom of the page.

90% of our received mail is SPAM or SPAM related. While we realize that blocked email is an inconvenience, we have chosen to error on the side of caution due to the possibility of inappropriate content slipping through and being seen by a student peering over a teacher’s shoulder.

If you have experienced this issue with email communication, we recommend that you check a few items noted below and try again.

1. Are you sure you have the correct address and that you did not mis-key?
2. Does your computer have current virus and spyware protection software installed and working properly?
3. Does your email contain embedded images (some signatures) or have a custom stationary look that utilizes images, sounds, and or other multi-media content?
4. Does your email address contain a correct return email address?
5. Are you trying to send the email as a blind copy?
6. Does your mail provider (or AOL, Hotmail, etc.) append anything to the message that might contain a phrase which could identify it as Spam?
7. Does your email have advertising in the body, header, or footer? e.g. "Find out more"
8. Does your email contain third party content in the form of html links or links in the header or footers of your email?
9. Does your email contain attached files?
10. Is the problem intermittent with sometimes email being delivered and other times it is not? If so, do you see any pattern such as messages go through if you reply to one they sent you, or they get blocked when you use an account which has a signature?
11. Did you get any notification indicating the message was undeliverable or didn’t go through?

- Virus Filter – Messages identified or suspect for Viruses, Trojans, and e-mail exploits will be deleted.
- DNS Blacklist - There are several servers on the internet that maintain a DNS Blacklist for servers know to distribute Spam or to have open relays which allow Spam. Our Filter uses those lists so if someone has an e-mail account on one of the Blacklisted servers then their mail will be blocked. It is their mail server owner who is responsible for being removed from those lists.
- Keyword Checking – There is a long list of keywords and phrases that if found in the subject or body of the message will be identified as Spam. Examples would include but not limited to phrases such as “don’t miss out”, “find out more”, “100% guaranteed”, “please answer quickly”, “call now”, “adult only”, and a host of obscene phrases. Words included would be Viagra, nympho, erotic, and all those words not fit to print. Yes, we know that not every message with one of those is Spam but these are the most common and if they are removed from the filter will let hundreds or thousands of Spam messages through each day.

- Header Checking – Messages will be blocked if the “From” field is empty, contains more than 4 numbers, or uses part of the recipient’s address/name. They will also be deleted if they have html scripts, contain remotely hosted images in the message body or if the message is mostly a graphic file with very little text. Both of those are methods Spammers use to get past the Keyword checking and often result in the obscene pics being displayed in the message. Messages that have false email headers and faulty return addresses will also be blocked.
- Macro Filter – Any files with Macros will be rejected and deleted, both incoming and outgoing. These are a potential security risk due to what could happen when a Word or Excel file is opened with a destructive Macro. Those are extremely easy for an end-user to create and then send to anyone with destructive results as soon as they open it.
- Bayesian – This is the “Smart” filter that uses algorithms to identify *potential* Spam. It results in a lot of false positives but the decision was made to delete all Bayesian identified messages instead of tagging them and sending them on through. This means that many thousands of messages are deleted each day and are not logged due to the size, so many legitimate messages are deleted as Spam and we have no way to trace what happened.
- Directory Harvesting – If someone sends a message that has several incorrect addresses in the “To:” field then the entire message will be rejected. This helps prevent Spammers from just sending a huge distribution list of potential names and getting lucky with some.
- Custom Blacklist – Individual mail addresses and entire mail domains can be added to a custom list to be blocked.
- File Attachments – Many types of files are blocked for security reasons and include those such as VBS, EXE, COM, BAT, and ZIP. Files such as XLS, PPT, DOC are NOT blocked *unless* they contain Macros. File attachments are quarantined so if they don’t have a Macro then they can be forwarded on to the recipient if they are work related and the recipient lets us know when they get an automated notification that it was blocked.