Internet Safety Policy

Introduction

It is the policy of SALAM SCHOOL to: (a) prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications; (b) prevent unauthorized access and other unlawful online activity; (c) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and (d) comply with the Children's Internet Protection Act [Pub. L. No. 106-554 and Utah State Uniform School Code]

Definitions - Key terms are as defined in the Children's Internet Protection Act (CIPA).

* Access to Inappropriate Material - To the extent practical, technology protection measures (or Internet filters shall be used to block or filter Internet, or other forms of electronic communications, access to inappropriate information. Specifically, as required by the Children's Internet Protection Act, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors.

* Subject to staff supervision, technology protection measures may be disabled or, in the case of minors, minimized only for bona fide research or other lawful purposes. To the extent practical, steps shall be taken to promote the safety and security of users of the SALAM SCHOOL online computer network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications.

* Specifically, as required by the Children's Internet Protection Act, prevention of inappropriate network usage includes: (a) unauthorized access, including so-called "hacking" and other unlawful activities; and (b) unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

Inappropriate Network Usage Supervision and Monitoring

* The employees in SALAM SCHOOL have a responsibility and obligation to take all reasonable measures to protect children and provide a safe online environment.

*Internet safety training is to be provided to minors that address:
•Appropriate online behavior
•Cyberbullying awareness and response
•Social networking sites
•Chat rooms
* It shall be the responsibility of all members of the SALAM SCHOOL staff to supervise and monitor usage of the online computer network and access to the Internet in accordance with this policy and the Children's Internet protection Act.

* Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of the Director of Technology or designated representatives.

CIPA DEFINITION OF TERMS:

TECHNOLOGY PROTECTION MEASURE. The term "technology protection measure" means a specific
technology that blocks or filters Internet access to visual depictions that are:

1. OBSCENE, as that term is defined in section 1460 of title 18, United States Code;

2. CHILD PORNOGRAPHY, as that term is defined in section 2256 of title 18, United States Code; or

3. Harmful to minors.

HARMFUL TO MINORS. - The term "harmful to minors" means any picture, image, graphic image file, or other visual depiction that:

1. Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;

2. Depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and

3. Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

SEXUAL ACT; SEXUAL CONTACT. - The terms "sexual act" and "sexual contact" have the meanings given such terms in section 2246 of title 18, United States Code.

Appropriate Use Policy for Computers and Network Resources

It is the belief of the SALAM SCHOOL that the use of technology for the purpose of information acquisition, retrieval, manipulation, distribution and storage is an important part of preparing children to live in the 21st century. The SALAM SCHOOL further believes that a "technology rich" classroom can significantly enhance both the teaching and learning process. This technology includes digital 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 SALAM SCHOOL believes guidelines regarding acceptable and appropriate use are warranted in order to serve the educational needs of students.

It shall be the policy of the SALAM SCHOOL 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 devices 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 SALAM SCHOOL Educational 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 appropriate use guidelines.

The district reserves the right to monitor, access, and disclose the contents of any user's files, activities, or communications.

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 SALAM SCHOOL that the Internet's advantages far outweigh its disadvantages. The SALAM SCHOOL 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 SALAM SCHOOL appropriate and acceptable use policy shall be subject to revocation of these privileges and potential disciplinary action.

Employee Appropriate Use Policy

Please read the following carefully. Violations of the Appropriate Use Guidelines may cause an employee's access privileges to be revoked, 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:

1. Staff must be aware that students have access to the Internet from all of the school systems' computers. Teachers must use good judgment and closely supervise their students' 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, he/she may be able to access sites that contain materials that are inappropriate for children or are not commensurate with community standards of decency. Students 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".

2. 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.

3. Never allow students to log in with a staff member's user name and password. With that information they could log in under the teacher name and look at private documents including e-mail and grades.

4. Be careful when entering your user name and password or changing your password. Do not allow students to look over your shoulder and have access to this information.

5. Never allow a student to use a computer unless they are logged on under their own name (K-2 students may use a generic "classroom account" created by the school ITS).

6. Enforce the Appropriate Use Guidelines while supervising students. It is the employee's responsibility to notify the administration of any violation of the Acceptable Use Policy.

7. Do not allow students to go to computer labs unsupervised.

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

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

10. The system requires employees to change passwords periodically. 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. Make sure any written password information is stored in a secure location. Do not leave passwords lying on your desk or in an unlocked drawer.

12. 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), and executable files. These types of email often contain viruses and can cause excessive network traffic or computing load. All employees must request permission from the building administrator before sending any messages to an entire school staff.

13. Employees must abide by the SALAM SCHOOL Web Site Posting guidelines when posting any materials to the web.

14. 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.

15. Employees and staff, maintaining or posting material to a Web site or blog that threatens a likelihood of substantial disruption in school, including harming or interfering with the rights of other students to participate fully in school or extracurricular activities is a violation of the Appropriate Use Policy.

Student Appropriate Use Policy

Please read the following carefully. Violations of the Appropriate Use Guidelines may cause a student's access privileges to be revoked for a period of time up to one school year, other disciplinary action, and/or appropriate legal action to be taken. It is expected that all students sign as having read the district AUP.

Any student who utilizes the computer lab(s) or any digital 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.

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:

1. Accessing, sending, creating or posting materials or communications that are:
a. Damaging to another person's reputation,
b. Abusive,
c. Obscene,
d. Sexually oriented,
e. Threatening or demeaning to another person,
f. Contrary to the school's policy on harassment,
g. Harassing, or Bullying
h. Illegal

2. Using the network for financial gain or advertising.

3. Posting or plagiarizing work created by another person without his/her consent.

4. Posting anonymous or forging electronic mail messages.

5. Attempting to read, alter, delete, or copy the electronic mail messages of other system users.

6. Giving out personal information such as phone numbers, addresses, driver's license or social security numbers, bankcard or checking account information.

7. 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.

8. Downloading, installing, or using games, music files, public domain, shareware or any other unauthorized program on any school's computer or computer system.

9. 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.

10. Gaining access or attempting to access unauthorized or restricted network resources or the data and documents of another person.

11. Using or attempting to use the password or account of another person or utilizing a computer while logged on under another user's account.

12. Using the school's computers or network while access privileges have been suspended.

13. 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.

14. Altering or attempting to alter the configuration of a computer, network electronics, the operating system, or any of the software.

15. Attempting to vandalize, disconnect or disassemble any network or computer component.

16. Utilizing the computers and network to retrieve information or run software applications not assigned by their teacher or inconsistent with school policy.

17. Providing another student with user account information or passwords.

18. Connecting to or installing any computer hardware, components, or software which is not school system property to or in the district's technology resources without prior approval of the district technology supervisory personnel.

19. 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.

20. Downloading or accessing via e-mail or file sharing, any software or programs not specifically authorized by Technology personnel.

21. Bypassing or attempting to circumvent network security, virus protection, network filtering, or policies.

22. Possessing or accessing information on school property related to "Hacking", or altering, or bypassing network security or policies.

23. Participating on message boards without teacher direction.

24. Students may use the school computer system only for legitimate educational purposes, which include class work and independent research that is similar to the subjects studied in school. Students shall not access entertainment sites, such as social networking sites or gaming sites, except for legitimate educational purposes under the supervision of a teacher or other professional.

25. All student use of the District network and Internet system or personal cell phones or other digital devices used by students while on campus is subject to the provisions of the individual school policies. Students may not share or post personal information about or images of any other student, staff member or employee without permission from that student, staff member or employee. If a student is found to have abused a personal cell phone or digital device in a manner that is not in accord with this Appropriate Use Policy, in addition to other disciplinary actions, the administrator may ban the students' use of any and all personal cell phone or digital devices.

26. Students should follow the guidelines for searching that utilize safe search engines and

technology.

27. Off Campus Internet Expression -- Students may be disciplined for expression on/off campus networks or websites only if the expression is deemed to cause a substantial disruption in school, or collide or interfere with the rights of other students, staff or employees.

28. Students maintaining or posting material to a Web site or blog that threatens a likelihood of substantial disruption in school, including harming or interfering with the rights of other students to participate fully in school or extracurricular activities is a violation of the Appropriate Use Policy and can subject the student to appropriate penalties and disciplinary action.

Web Site Posting Guidelines

I. Student Information, Work, and Pictures:

1. Web pages hosted from SALAM SCHOOL's web services may contain a reference to a student. This includes references to students in photographs or in text.

2. The following student information is appropriate 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. 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., 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 requests to have their personal email address listed in the appropriate area on the schools' 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 SALAM SCHOOL's provider).

4. Links to "non-official" SALAM SCHOOL 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.

IV. Maintaining or posting material to a Web site or blog that threatens a likelihood of substantial disruption in school, including harming or interfering with the right of other students to participate fully in school or extracurricular activities is a violation of the Appropriate Use Policy, and can subject the student, staff, or employee member to appropriate penalties and disciplinary action.

V. Compliance with SALAM SCHOOL Appropriate Use Guidelines

All material posted to the SALAM SCHOOL website(s) must adhere to all provisions set forth in the Appropriate Use Guidelines. Items from these documents, which are relevant to information posted on the web, are the following:

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 SALAM SCHOOL 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, driver's 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.

VI. 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 on the enrollment data form and is cross-referenced in the student information system.