ACCEPTABLE USE OF TECHNOLOGY AND INTERNET SAFETY POLICY

SURRY COUNTY PUBLIC SCHOOLS

All use of the Surry County School Division's computer system shall be consistent with the School Board's goal of promoting educational excellence by facilitating resource sharing, innovation and communication. The term computer system includes hardware, software, date, communication lines, and devices, terminals, printers, CD-ROM devices, tape or flash drives, servers, mainframe and personal computers, tablets, cellular phones, smart phones, the Internet and any other internal or external network.

I. Computer System Use-Terms and Conditions:

1. **Acceptable Use.** Access to the Division's computer system shall be (1) for the purposes of education or research and be consistent with the educational objectives of the Division or (2) for legitimate school business.

2. **Privilege.** The use of the Division's computer system is a privilege, not a right.

3. **Unacceptable Use.** Each user is responsible for his or her actions on the computer system. Prohibited conduct includes:

   - Using the network for any illegal or unauthorized activity, including violation of copyright or contracts, or transmitting any material in violation of any federal, state or local law.
   - Sending, receiving, viewing or downloading illegal material via the computer system.
   - Unauthorized downloading of software.
   - Downloading copyrighted material for unauthorized use.
   - Using the computer system for private financial or commercial gain.
   - Wastefully using resources, such as file space.
   - Gaining unauthorized access to resources or entities.
   - Posting material authorized or created by another without his or her consent.
   - Using the computer system for commercial or private advertising.
   - Submitting, posting, publishing or displaying any obscene, profane, threatening, illegal or other inappropriate material.
   - Using the computer system while access privileges are suspended or revoked.
   - Vandalizing the computer system, including destroying data by creating or spreading viruses or by other means.

- Intimidating, harassing, bullying or coercing others.
- Threatening illegal or immoral acts.

4. **Network Etiquette.** Each user is expected to abide by generally accepted rules of etiquette, including the following:

    - Be polite.
    - Users shall not forge, intercept or interfere with electronic mail messages.
    - Use appropriate language. The use of obscene, lewd, profane, threatening or disrespectful language is prohibited.
    - Users shall not post personal contact information, other than directory information as defined in Policy JD Student Records about themselves or others. This including names, home, school or work addresses, telephone numbers, or photographs, about themselves or others.
    - Users shall respect the computer system's resource limits.
    - Users shall not post chain letters or download large files.
    - Users shall not use the computer system to disrupt others.
    - Users shall not read, modify or delete data owned by others.

5. **Liability.** The School Board makes no warranties for the computer system it provides. The School Board shall not be responsible for any damages to the user from use of the computer system, including loss of data, non-delivery or missed delivery of information, or service interruptions. The School Division denies any responsibility for the accuracy or quality of information obtained through the computer system. The user agrees to indemnify the School Board for any losses, costs or damages incurred by the School Board relating to or arising out of any violation of these procedures.

6. **Security.** Computer system security is a high priority for the school division. If any user identifies a security problem, the user shall notify the building principal or system administrator immediately. All users shall keep their passwords confidential and shall follow computer virus protection procedures.

7. **Vandalism.** Intentional destruction of or interfere with any part of the computer system through creating or downloading computer viruses or by other means is prohibited.

8. **Charges.** The School Division assumes no responsibility for any unauthorized charges or fees as a result of using the computer system, including telephone, data or long-distance charges.

9. **Electronic Mail.** The School Division's electronic mail system is owned and controlled by the School Division. The School Division may provide electronic mail to aid students and staff if fulfilling their duties and as an education tool. Electronic mail is not private. Students' electronic mail can be monitored. The electronic mail of staff may be monitored and accessed by the School Division. All electronic mail may be archived. Unauthorized access to an electronic mail account by any student or employee is prohibited. Users may be held personally liable for the content of any electronic message they create or that is created under their account or password. Downloading any file attached to an electronic message is prohibited unless the user is certain of the message's authenticity and the nature of the file.

10. **Enforcement.** Software will be installed on the Division's computers having Internet access to filter or block internet access through such computers to child pornography and obscenity. The online activities of users may also be monitored manually. **Any violation of these regulations shall result in loss of computer system privileges and may also result in appropriate disciplinary action, as determined by School Board policy, or legal action.**

II. Internet Safety

The School Division will integrate Internet Safety into the K-12 curriculum and instruction. The Internet is a valuable tool and the Virginia Department of Education and the School Division will take the necessary steps to ensure that the students learn how to use the Internet safely and effectively.

1. **Personal Safety on the Internet**
   - Students should never give out personal information without an adult's permission.
   - Students should understand that predators are always present on the Internet and recognize the various forms of cyber bullying and know what steps to take if confronted.

2. **Information on the Internet**
   - Students and parents should discuss how to identify acceptable sites and what to do if an inappropriate site is accessed.
   - Students should be aware of Web advertising and realize not all sites provide truthful information.

3. **Activities on the Internet**
   - Students and parents should discuss acceptable social networking and steps to take when encountering a problem.
   - Students and parents should be aware of potential dangers of emailing, downloading files and peer-to-peer computing. These could lead to viruses, legal issues, harassment, sexual predators or identity theft.

4. **Protecting Yourself**
   - Students and parents are required by law to report illegal Internet communication and activities to Internet Service Providers and local law enforcement authorities.
   - Students and parents should use caution when visiting chat rooms and using instant messaging (know with whom you are communicating).

III. Resources to help students and parents remain safe on the Internet

a. **Get Your Web License (PBS KIDS)** **http://pbskids.org/license**
b. **Tips by Teens for Teens (GetNetWise)**
   http://kids.getnetwise.org/safetyguide/teens
c. **KeepSafe Internet Safety Coalition**
   http://ikeepsafe.org/iksc_statemessage/state.php?abbr=VA
d. **NetSmartz: National Center for Missing and Exploited Children**
   http://www.netsmartz.org
e. **Stay Safe Online: National Cyber Security Alliance**
   http://www.staysafeonline.org/

Legal Ref.: Guidelines and Resources for Internet Safety in Schools

Adopted: August 13, 2013

Legal Refs: 18 U.S.C. §§ 1460, 2256.
47 U.S.C. § 254.

Code of Virginia, 1950, as amended, §§ 18.2-372, 18.2-374.1:1, 18.2-390, 22.1-70.2 and 22.1-78.

Guidelines and Resources for Internet Safety in Schools, Virginia Department of Education (Second Edition October 2007)

Cross Refs:

GCPD	Professional Staff Discipline
JFC	Student Conduct
JFC-R	Standards of Student Conduct

ACCEPTABLE USE OF TECHNOLOGY AND INTERNET SAFETY
STUDENT/PARENT CONSENT FORM

SURRY COUNTY PUBLIC SCHOOLS

The Internet is a powerful tool that should be used wisely!

The students enrolled in Surry County Public Schools have access to the District computers, the network and technology for educational purposes. We have filtering software in place but we cannot guarantee that access to all inappropriate materials will be blocked. Access to District technology is a privilege, not a right. Surry County Public Schools' electronic network is part of the curriculum and is not a public forum for general use.

Attached you will find our Acceptable Use of Technology and Internet Safety Policy. Please read this policy carefully and understand to gain access to the Internet, all students must sign and return this form. Students under the age of 18 must also obtain parental consent. Detach and keep a copy of the policy for your records before signing and returning this consent form to your child's school.

STUDENT CONSENT

I understand that my computer use is a privilege and **NOT** a right and is **NOT** private. The Division will monitor my activity on the computer system.

I have read the Acceptable Use of Technology and Internet Safety Policy and I agree to abide by these rules. I understand that violation of the policy may result in disciplinary action, including loss of privileges, suspension or expulsion.

Student's name (print):_____

Student's signature: _____ Date: _____

PARENTAL CONSENT

I have read the Acceptable Use of Technology and Internet Safety Policy. I understand that it is a privilege for my child to use the Division's electronic communications system and in consideration for having access to the public network, I understand that is it my child's responsibility to abide by all rules and regulations of this Acceptable Use of Technology and Internet Safety Policy. I further understand that violation of the policy may result in disciplinary action including loss of privileges, suspension, or expulsion of my child.

___ I give permission for my child to participate in the Division's electronic communication system and certify that the information contained on this form is correct.

___ I do NOT give permission for my child to participate in the Division's electronic communication system and certify that the information contained on this form is correct.

Parent/Guardian's Name (print):_____

Parent/Guardian's Signature: _____

Name of Student (print):_____

Address: _____

Home telephone: _____