Internet Safety Program

Keeping our students safe!

Approved 2008
INFORMATIONAL

TO: Division Superintendents
FROM: Billy K. Cannaday, Jr.
Superintendent of Public Instruction

SUBJECT: Guidelines for Internet Safety Instruction in Schools

Legislation approved by the 2006 General Assembly and signed by Governor Kaine requires the addition of a student Internet safety component to division Acceptable Use Policies (AUP). This legislation can be found at the following address: http://leg1.state.va.us/cgi-bin/legp504.exe?061+ful+CHAP0052+pdf.

The legislation requires Internet safety to be integrated within each school division’s academic instructional program. It also directs the Superintendent of Public Instruction to issue guidelines regarding Internet safety instruction.

The purpose of this memorandum is to disseminate the department’s guidelines and related resources to implement this legislation. The document, Guidelines and Resources for Internet Safety in Schools, is available in PDF format for school divisions to print and duplicate as needed. The document can be accessed from the department’s Web page: http://www.doe.virginia.gov/VDOE/Technology/OET/Internet-safety-guidelines.shtml. At a later date, the department will issue companion documents related to the integration of Internet safety within curriculum and instruction.

Division Superintendents currently are required to submit an updated AUP biennially: http://www.doe.virginia.gov/VDOE/suptsmemos/2001/inf153.html. The Internet safety component must be included in the September 2008 submission. During school year 2006-2007, the division's Internet safety policy should be developed, aligned with the
state guidelines, and incorporated into the AUP. By June 1, 2007, each division must send a statement to the director of the Office of Educational Technology confirming the completion of this work. During school year 2007-2008, the division will review the progress and effectiveness of its Internet safety policy and the implementation of its Internet safety program. By September 1, 2008, each division must submit to the department a copy of the AUP, including the Internet safety policy, and a statement that the AUP and Internet safety program have been reviewed. The department will review division policies for compliance in September 2008.

The Bedford County (Va.) Sheriff’s Office, under the leadership of Sheriff Michael J. Brown and through the Operation Blue Ridge Thunder Program, has arranged for Virginia school divisions to access NetSmartz materials from the National Center for Missing & Exploited Children. These materials will help divisions implement Internet safety programs. Downloadable versions of this material are available on the NetSmartz’s Web page: http://www.netsmartz.org/education/.

Delegate Fralin has proposed House Joint Resolution No. 5135 designating September—in 2006 and each succeeding year—as Internet Safety Month in Virginia. To review this joint resolution, see http://leg1.state.va.us/cgi-bin/legp504.exe?062+ful+HJ5135.

Questions about the department’s guidelines should be addressed to Dr. Tammy McGraw, director of the Office of Educational Technology, at (804) 225-4429 or at tammy.mcgraw@doe.virginia.gov.
Be it enacted by the General Assembly of Virginia:

1. That § 22.1-70.2 of the Code of Virginia is amended and reenacted as follows:

§ 22.1-70.2. Acceptable Internet use policies for public and private schools.

A. Every two years, each division superintendent shall file with the Superintendent of Public Instruction an acceptable use policy, approved by the local school board, for the international network of computer systems commonly known as the Internet. At a minimum, the policy shall contain provisions that (i) are designed to prohibit use by division employees and students of the division's computer equipment and communications services for sending, receiving, viewing, or downloading illegal material via the Internet; (ii) seek to prevent access by students to material that the school division deems to be harmful to juveniles as defined in § 18.2-390; (iii) select a technology for the division's computers having Internet access to filter or block Internet access through such computers to child pornography as set out in § 18.2-374.1:1 and obscenity as defined in § 18.2-372; and (iv) establish appropriate measures to be taken against persons who violate the policy; and (v) include a component on Internet safety for students that is integrated in a division's instructional program. The policy may include such other terms, conditions, and requirements as deemed appropriate, such as requiring written parental authorization for Internet use by juveniles or differentiating acceptable uses among elementary, middle, and high school students.

B. The superintendent shall take such steps as he deems appropriate to implement and enforce the division's policy.

C. On or before December 1, 2000, and biennially thereafter, the Superintendent of Public Instruction shall submit a report to the Chairmen of the House Committee on Education, the House Committee on Science and Technology, and the Senate Committee on Education and Health which summarizes the acceptable use policies filed with the Superintendent pursuant to this section and the status thereof.

D. In addition to the foregoing requirements regarding public school Internet use policies, the principal or other chief administrator of any private school that satisfies the compulsory school attendance law pursuant to § 22.1-254 and accepts federal funds for Internet access shall select a technology for its computers having Internet access to filter or block Internet access through such computers to child pornography as set out in § 18.2-374.1:1 and obscenity as defined in § 18.2-372.

E. The Superintendent of Public Instruction shall issue guidelines to school divisions regarding instructional programs related to Internet safety.

2. That, within 45 days of the enactment of this act, the Superintendent of Public Instruction shall issue a superintendent's memorandum advising school divisions of the provisions in this act and encourage cooperation with local law-enforcement agencies in its implementation.
Purpose: To define and describe the board’s acceptable use policy for computer systems and network resources by students, board members, and staff

Definitions

Computer Systems - Any combination of hardware, software, data, communication lines and devices, terminals, printers, CD-ROM devices, tape drives, servers, mainframe, personal computers or any other computer related equipment, peripherals or software owned or leased by the board.

Cyberbullying - Threats made by one computer system user toward another through electronic-mail, text messaging or posts made on Web sites (e.g., web-logs (commonly referred to as "blogs"), social networking sites, chat rooms, etc.

Internet Safety - Required content, within the division’s curriculum and instruction program, defining roles and responsibilities for all computer resource stakeholders, safety measures, data and network security plans, safety breach procedures, evaluation plans, professional development, and community outreach programs.

Network Resources - Printing services, computer programs, data files, data storage, Internet access and functions available to a user from computers systems that are not owned by the division.

User - An individual who is accessing or may access the division’s computer system and/or network resources either from within the division or outside the division via the Internet.

The division shall operate its computer systems and access its network resources in compliance with federal, state, and local laws and regulation for the acceptable and safe use of such systems and resources.

The superintendent/designee shall review this policy every two years, submit a copy of the approved policy to
the State Superintendent of Public Instruction, and cause any changes to be disseminated to the division’s computer systems' users.

**Applicable Guidance**

1. The division’s computer systems must be used (1) in support of education and/or research, or (2) for legitimate school business. Use of the computer system is a privilege, not a right. Any communication or material used on the computer system, including electronic mail or other files deleted from a user’s account, may be monitored or read by school officials.

2. The superintendent/designee shall establish regulation(s) associated with this policy for board review, providing administrative procedures detailing the safe and appropriate uses, ethics and protocol for the computer system. These procedures shall include:
   a. Prohibition against use by division employees and students of the division’s computer equipment and communications services for sending, receiving, viewing, or downloading illegal material via the Internet;
   b. Provisions, including the selection and operation of a technology protection measure for the division’s computers having Internet access to filter or block Internet access through such computer, that seek to prevent access to:

   (1). Child pornography as set out in Virginia Code § 18.2-374.1:1 or as defined in 18 U.S.C. § 2256;
   (2). Obscenity as defined by Virginia Code § 18.2-372 or 18 U.S.C. § 1460; and
   (3). Material that the division deems to be harmful to juveniles as defined in Virginia Code § 18.2-390, material
that is harmful to minors as defined in
47 U.S.C. § 254(h)(7)(G), and material that is otherwise inappropriate for minors.
c. Provisions establishing that the technology protection measure is enforced during any use of the division’s computers by minors;
d. Provisions establishing that the online activities of minors will be monitored;
e. Provisions designed to protect the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications. In particular, students will be strictly prohibited from using the division’s computer system and network resources to:

(1). Engage in activities prohibited by federal, state, or local law, ordinance, or regulation, including unauthorized access and/or hacking or engage in harassment (cyber bullying) by computer or technology-based devices; and/or,

(2). Disclose, use, or disseminate personal information regarding minors, except as is authorized by law or by consent.
f. Provisions designed to prevent unauthorized online access by minors, including “hacking” and other unlawful activities by minors online;
g. Provisions prohibiting the unauthorized disclosure, use, and dissemination of personal information regarding minors; and

h. Internet safety component for students that is integrated in the division’s instructional program.
3. Use of the division’s computer system shall be consistent with its educational or instructional mission or administrative function as well as the varied instructional needs, learning styles, abilities and developmental levels of students. The division’s computer system is not a public forum.

4. Signature acknowledgement of compliance with this policy by every user, including:
   a. Every student and parent/guardian of each student shall sign the Acceptable Computer System Use Agreement contained in the regulation associated with this policy, before using the division’s computer system.
   b. Every employee contract of the division shall include compliance with the Acceptable Use Agreement as an element of that employment contract.

5. Failure of any student, teacher, administrator or other employee of the division to follow the terms of the Acceptable Use Agreement, this policy or accompanying regulation may result in loss of computer system privileges, disciplinary action, and/or appropriate legal action.

   a. Consequences for Inappropriate Use for Students
      Minimum of short-term suspension of 10 days, or less, with the balance of any days to be served carrying over to the succeeding school year, and/or loss of computer and Internet privileges to maximum of expulsion. Additionally, the matter shall be reported to the superintendent/designee and shall also be reported to the Sheriff’s Department if the potential exists for criminal charges to be filed.

   b. Consequences for Inappropriate Use by Employees
      Employees who violate the Acceptable Use Policy are subject to discipline as deemed necessary. Employee discipline may include, but shall not be limited to
verbal reprimand, letter of reprimand, suspension with or without pay, to termination. Additionally, the matter shall be reported to the superintendent/designee and shall also be reported to the Sheriff’s Department if the potential exists for criminal charges to be filed.

6. The board is not responsible for any information that may be lost, damaged or unavailable when using the computer system or for any information retrieved via the Internet. Furthermore, the board will not be responsible for any unauthorized charges or fees resulting from access to the computer system.

7. The superintendent/designee shall submit to the Virginia Department of Education this policy and accompanying regulation biennially.

Comments

Questions about this policy should be directed to the Chief Technology Officer, Stafford County Public Schools, 31 Stafford Avenue, Stafford, Virginia 22554.

Adopted: 06/24/08

_______

PURPOSE: To describe the parameters of acceptable use

As a condition of student access to the Internet and prior to such access on school computers and hardware a written instrument executed by the student and the student’s parent/guardian must be on file with the school which sets forth the terms and conditions of Internet use, rules of on-line behavior, and access privileges.

Every employee contract of the division shall include compliance with the Acceptable Use Agreement as an element of that employment contract.

Acceptable Use includes:

- The agreement of the parent and student/employee that use of school owned computers, hardware, and software, and access of the Internet using same, is a privilege, not a right, and may be forfeited upon failure of the student/employee to adhere to the terms of the agreement;
- The consent of the parent for the student to use school computers, hardware, and software to access the Internet;
- That although the division employs constant filtering technology and building monitoring to prevent access to child pornography, obscenity, and other harmful material, the parent/employee absolves the school of any liability or responsibility should the student/employee be exposed to offensive material on the Internet;
- That the student shall abide by all provisions of the student code of conduct pertaining to computers and use of related hardware and software, or may forfeit the privilege to use school computers, hardware and software, and to access the Internet; employees will abide by elements of this agreement as noted as well as the division’s Acceptable Use Policy;
• The agreement of the parent, student/employee that the student/employee shall not contractually obligate the board, school, school official, or any person for any services, products, etc., which may be available through and offered over the Internet and that if the student/employee should so obligate the board, school, school official, or person, that the parent/employee shall assume full financial responsibility and shall indemnify, defend, and hold the board, school, school official harmless;
• The agreement of the student/employee not to use the Internet for any illegal purpose;
• The agreement of the student/employee not to send any abusive, profane, or obscene language over the Internet;
• The agreement of the student/employee to adhere to accepted school rules of courtesy and etiquette when accessing the Internet;
• The agreement of the student/employee to not disclose to any other person his password, account number, etc., or to disclose that of any other person;
• The agreement of the student/employee not to use school computers, hardware, and/or software, or the Internet, to engage in any activity which violates the policies, regulations, and rules of the board or school to include but not limited to hacking, harassment, or cyber bullying.
• The agreement of the student/employee that he shall not violate the policies or regulations of the Internet Access Provider.

In the event that a student/employee violates the terms of the acceptable use agreement or in the case of students, the provisions of the Code of Student Conduct pertaining to computers and use of related hardware and software, the administrator may, in addition to or in
lieu of any other disciplinary measure which he may impose, rescind the privilege of the offending student/employee to use school computers, hardware, software, and/or to access the Internet.

A student/employee may apply to the administrator for restoration of such privileges and, should their request be denied by the administrator, may appeal that decision to the superintendent/designee by filing a written appeal within seven (7) calendar days of receiving the written decision of the administrator.
Internet Safety Component

Philosophy

A superior instructional program is a top priority of the School Board, administration, staff and faculty. The Stafford County school system focuses on strategies that challenge each student to reach his or her potential and to prepare each student to succeed in society. We seek to promote student access to and use of computers, the network and related technology. To that end the privilege, but not the right, is extended to students to use school computers and when appropriate, to access the Internet and to communicate electronically. The ultimate goal of technology integration is to ensure that each child leaves our schools with the skills and knowledge necessary to enable him/her to aspire to the highest levels of achievement in chosen endeavors and become a contributing member of our democratic society.

As part of our effort to ensure that our students are provided a safe environment in which to learn and grow, we have created this Internet Safety Program. This Program seeks to help students learn the power of the Internet and how to maximize its use for learning and minimize its dangers.

Roles and Responsibilities

All roles and responsibilities will be reviewed annually as part of the overall evaluation of the program. Roles and responsibilities will be updated as needed to promote student safety. (See Evaluation section for details.)

Administrators:
• Enforce AUP and adhere to discipline guidelines in the Student Code of Conduct and AUP
• Respond to any cyberbullying claims
• Be knowledgeable about Internet safety and stay current
• Make sure teachers are monitoring students' use of school computers and other technologies, and covering Internet safety skills in their lessons as needed
• Seek input from staff and community regarding filtering

Teachers:
• Be familiar with and report all claims of cyberbullying
• Monitor student Internet and other computer/technology use
• Report AUP violations to administrators
• Include Internet safety concepts in taught curriculum and when using technology with students
• Be familiar with provisions of and monitor for violations of copyright and ethics standards as regards to the use of technology and the Internet

Technology Resource Teachers:
• Be familiar with and report all claims of cyberbullying
• Train instructional staff on Internet safety concepts
• Train teachers on proper monitoring of students
• Reinforce Internet safety concepts in computer clubs and other opportunities when working with students
• Provide resources to teachers and community members on Internet safety
Library Media Specialists:
- Be familiar with and report all claims of cyberbullying
- Reinforce Internet safety during library orientations
- Monitor student Internet and other computer/technology use in the library
- Train teachers and students on copyright standards

Building level Resource Officers:
- Respond to violations of AUP that involve illegal acts
- Be familiar with and monitor Internet safety allegations
- Offer training on legal ramifications to staff if needed

School Counselors:
- Be familiar with and report all claims of cyberbullying
- Offer additional resources to students, parents and teachers on Internet safety and cyberbullying

Computer Technician/Trainers:
- Monitor network and Internet at administrators' direction
- Report any potential AUP violations to administration
- Work with administration to block known harmful sites beyond the applied filter
- Report uncategorized sites to filter software vendor for future filtering purposes

Instructional Technology and Information Services Staff:
- Maintain filtering technology for all Internet traffic and seek input from schools regarding additional filtering requirements
- Provide Internet safety concepts to all teachers and instructional staff
- Provide training as necessary to administrators and technical staff
- Serve as a liaison between VDOE and the division
- Evaluate effectiveness of Internet Safety Program and implement any needed adjustments/modifications/trainings as determined necessary for program success

Students:
- Abide by the Acceptable Use Policy and the Student Code of Conduct
- Report AUP violations to the administration
- Report instances of cyberbullying to the administration
- Learn and understand the dangers of the Internet and strive to be safe when online

Community Stakeholders:
- Take opportunities to attend Internet safety training at schools
- Volunteer to serve on the Technology Advisory Committee
- Provide feedback to the Technology Advisory Committee about issues and topics related to the Internet Safety Program
- Volunteer expertise in the area of Internet safety to schools
Filtering and Monitoring Procedures

The program specifies filtering and monitoring of all Internet traffic from all Stafford County Public School sites including school buildings and administrative sites. The filter configuration is managed by its associated school’s administrative staff in coordination with the community it serves.

Multiple tiers of monitoring occur at the Division, School and individual computer levels. Real time statistics, remote view/control of computers, and logging of all traffic are used to monitor student and staff activity online. For filtering, each individual school has an appliance operating in client mode to a central management appliance as the control device. School staff manages filtered categories by individual school site. Central Technology staff provides support and training. Pornography and child pornography sites are filtered at all sites for all computers and users. The subscription service provided for these appliances update the filter categories within 24 hours of new web sites being identified.

A network proxy server is used for logging and statistical analysis of Internet traffic. All computers are blocked by a firewall from access to the Internet unless the request is made using these proxy servers. Policy-based desktop management tools are used to remote view/control individual computers as needed.

Stafford County Public Schools’ technology staff will stay abreast of current and emerging technologies that may affect our filtering and monitoring capabilities. The continued training and research of our staff is vital to the continued success of our Internet filtering processes.

Data and Network Security

The Department of Instructional Technology and Information Services manages all data and network security measures. Methods to ensure data and network security are reviewed throughout each year to monitor areas of weakness and to determine ways to address those weaknesses. The community based Technology Advisory Committee is given updates at least annually on current updates and changes to network security protocols. IT/IS staff are trained and current on all updates. Staff engineers are assigned the responsibility to review and stay current on network security protocols. Training is made available and attended on an annual basis.

Procedures to Address Breach of Security and/or Safety

All minor security and safety breaches are handled at the school level by school staff and administrators. Minor breaches might include students accessing inappropriate websites or teachers not logging off the computer and giving students access to their network accounts. These breaches are dealt with by using the guidelines in our AUP and Student Code of Conduct.

All major security and safety breaches are handled at the district level by the Department of Instructional Technology and Information Services in conjunction with the district Superintendent. Major breaches are those that might include loss of service or loss of data. If the breach violates local, state or federal laws, then outside agencies are sought out for help. SCPS uses network monitoring as part of our security design and has backup data systems in place as well. All network engineers are also trained on how to retrieve evidence if needed.

Documentation of any such incident is kept by the Department of Instructional Technology and Information Services. If student discipline is involved, documentation is kept at the school level as well. If staff discipline is involved, documentation is kept by the Human Resources Department.
**Professional Development**

Stafford County Public Schools’ goal is that all students understand the following concepts regarding Internet safety:

- The Internet is a powerful tool that should be used wisely.
- Not all Internet information is valid or appropriate.
- Strive to maximize the Internet’s potential while protecting themselves.
- Internet messages or the people who send them are not always what or who they seem.
- Predators and cyberbullies anonymously use the Internet to manipulate students – students must learn how to avoid dangerous situations and get adult help.
- Internet activities can be enjoyable and rich in learning, however, students need to know which activities are safe and legal.

Stafford County Public Schools’ goal is that all teachers are trained on how to educate students about the Internet safety concepts listed above. Training for teachers and instructional staff will include the concepts for students as well as covering these instructional technology use concepts:

- Classroom Internet use can be exciting, rewarding, and challenging. Students’ Internet use should be age appropriate.
- Monitoring students is crucial.
- Students’ technological interactions in the virtual world can be negative and spill over into the real world.
- Exchanging information with others is a great way to use the Internet but also possesses inherent dangers.
- Students need to hear the rules often

All teachers are surveyed at the start of each school year to determine the need for training. In the Fall of 2007, all SCPS teachers were trained in the basics of Internet safety and how to educate their students. Each fall, SCPS will survey teachers and again provide training based on needs.

Stafford County Public Schools will assess students’ learning about these Internet safety concepts by surveying sample groups of students.

**Community Outreach**

The Internet Safety program is a priority of our Technology Advisory Committee who seek to promote the sharing of information on this and other topics. SCPS shares information about Internet safety on our school websites and in school newsletters. We also use the curriculum from Connect with Kids© to work with students and families on bullying and other character education topics. Many of our schools offer training and information sessions for parents on Internet Safety and our local Sherriff’s office has been involved in helping train parents as well. SCPS also includes Internet safety literature and information at our Instructional Technology Exchange and other public events for the community.

Future goals include sharing information via our new community-access television broadcast station on the local cable channel and sharing more SCPS based materials with the community.
Feedback will be solicited via our district website and through parent organizations. The feedback will be collected and shared with the evaluation team in the spring of each year. The feedback will help us to revise our program as needed and to assess our impact on educating the community.

**Acceptable Use Policy Revisions and Updates**

The Supervisor of Instructional and Assistive Technology is the primary point of contact and coordinates all division plans and programs related to Internet safety.

The Department of Instructional Technology and Information Services, with the assistance of the Technology Advisory Committee, will conduct an annual, independent evaluation of the Acceptable Use Policy and Internet Safety Program. This evaluation will complete in May of each year, and the results presented to the school board by the Technology Advisory Committee in conjunction with their annual evaluation of the district's technology plan.

This evaluation will include, but not be limited to:

- Detailed review of individual roles and responsibilities as pertains to this program;
- Review of trends for numbers and severity of AUP violations and an audit of associated disciplinary penalties awarded to ensure consistency with the AUP guidelines;
- Review data for security violations since the last evaluation with particular attention to the details for any major security breaches and any involving unlawful acts to determine what, if any, modifications are required to the current program and policy;
- Review of all stakeholder comments and feedback received since the last evaluation on Internet Safety Program and AUP issues;
- Review current VDOE guidelines and state legislation against current program to ensure consistency with higher authority;
- Review selected curricula and lesson plans gathered from the schools for content and effectiveness;
- Review of sample population student assessment results.

As a result of this evaluation, the Department of Instructional Technology and Information Services will determine the need for program/policy changes, and if warranted, will prepare the required change documents for School Board approval in accordance with the district Policy and Regulations Manual such that they are in place prior to the start of the next school year. If, as a result of this evaluation, it is determined that no such modifications are required, the department will make a positive, formal report of that fact to the School Board.

School Board presentation: The Internet safety program is presented formally to the School Board and also made available at community outreach events. The community based Technology Advisory Committee receives update on Internet Safety as part of our review of Instructional Technology accomplishments.
Documentation:
AUP and Internet Safety policy are located on our website at www.staffordschools.net.

Implementation and Adjustment:
2007-2008
June 2007 - Stafford County Public Schools updated the Acceptable Use Policy to include information regarding our Internet safety policy.
September 2007 – All Stafford County Public Schools’ teachers were trained on the Internet safety concepts identified by the Virginia Department of Education.
September 2007 - Stafford County Public Schools shared K-12 technology benchmark skills with all teachers that included Internet safety concepts.
During the school year – teachers trained students about Internet safety and planned lessons that integrated Internet safety concepts into their instruction and schools shared Internet safety resources and training with parents and community members.
April 2008 – Internet safety materials and instructional information were shared at the community event, our Instructional Technology Exchange
May 2008 – July 2008– The Department of Instructional Technology and Information Services began reviewing progress made over the school year and created the final Internet Safety Program guide to present to the School Board for approval.

2008-2009
Stafford County Public Schools will implement the updates and revisions to our Internet safety program and continue to evaluate their effectiveness in an effort to keep all our students safe.