Stafford County Public Schools
Acceptable Computer Use Policy #6301

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 an Acknowledgement of Receipt document which includes agreement to abide by the Acceptable Computer Use Policy.

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. <u>Consequences for Inappropriate Use for Students</u>

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 Executive Director for Technology Services, Stafford County Public Schools, 31 Stafford Avenue, Stafford, Virginia 22554.

Adopted: 06/24/08
Amended by School Board: 06/14/11
Reviewed: 04/15/13
Readopted: 12/12/13
****

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