

SUMMARY OF COMPUTER USE POLICY
Article 22 of the SLCS D Policies
Adopted 3/06/02

Section 22.1 Purpose

To promote the use of computers, including the Internet and computer-related technology, as educational and research tools; encourage the use of computers and computer-related technology to advance and promote learning and teaching; and establish controls to prevent the misuse, impairment, disruption, and damage to the District computer system or any of its components.

Section 22.2 Definitions

“Computer System” or “system” means all computer hardware, equipment, software, cables and wires, as well as electronic mail and internet services and connections, and network facilities.

“Electronic Mail” (email) means electronic transfer of information in the form of electronic messages and documents from a sending party to one or more receiving parties via the computer system.

“Network Coordinator” means the person designated by the Superintendent to supervise, manage and direct the administration, design, operation and use of the computer system.

Section 22.3 Computer System Administration

The Network Coordinator:

- designs, manages and supervises the operation and use of the computer system;
- monitors all network activities to ensure proper use of the system;
- interprets District policy and regulations governing use of the computer system;
- provides employee training for proper use of the computer system;
- ensures that all disks and software loaded onto the computer network have been scanned for computer viruses; and
- is responsible for determining and controlling access to the District computer system.

Section 22.4 Privacy and Retention of E-mail and Internet Transmissions & Records

All e-mail and internet transmissions and records:

- are not the personal or private property of any user, and students and staff should not expect, nor does the District guarantee, privacy for e-mail or any use of the system;
- may be accessed, monitored and viewed by the District;
- may be subject to disclosure in court proceedings and to the public under the Freedom of Information Law; and
- shall be removed and deleted regularly, and the Network Coordinator may remove/delete any more than 30 days old.

Section 22.5 District Rights

The School District:

- reserves the right to monitor use of the computer system;
- assumes no responsibility or liability for deleted or lost files;
- reserves the right to remove a user from the computer system;
- shall not be responsible for:
 - any information obtained by a user, such information being obtained at the user's sole and exclusive risk,
 - any damages, including but not limited to the loss of data whether or not caused by negligence, errors or omissions of the District,
 - any costs, liabilities or damages incurred by the user;
- is not responsible for any viruses, worms or cookies imparted to a user's home computer from the District's computer system; and
- reserves and retains the right to amend, modify or change this policy.

Section 22.6 Access to System

- Only authorized users will be granted access;
- Each authorized user will have only one unique User ID and one password (changed periodically) which shall not be given to any other official, employee or student except as otherwise provided in the policy;
- Log-in to the system shall only occur when the user is in the immediate vicinity of the computer terminal, and the user shall log off the network when leaving the terminal or area for any reason or time period;
- The Network Coordinator shall be notified whenever the system refuses to allow access to any site following four consecutive unsuccessful log-in attempts, and no further access shall be granted or permitted except by the Network Coordinator; and
- Authorization for access shall terminate for:
 - an official or employee when he/she leaves District employment
 - a student when he/she is no longer enrolled in the District
 - any user when he/she is no longer is authorized to have access.

Section 22.7 Internet Access By Students

Students:

- will be provided with access to the internet only during the school day whether in or out of class, but only after receiving training and their user ID and password
- will be provided with individual accounts and e-mail addresses
- may, subject to monitoring by a District official or staff member browse the world wide web, read news groups, construct their own web pages using District computer resources, and belong to approved mailing lists.

Section 22.8 Acceptable Use & Conduct

- Use of the computer system and/or any component thereof, shall be in strict conformance with the following:
- Use of and access to the computer system shall only be for the educational instruction and advancement of students, and for District officials/staff to conduct official District business;

- No unauthorized software shall be permitted to be installed or used on the system;
- Personal software will only be allowed on the computer system, or any component part thereof, provided that the software is licensed, approved by the Network Coordinator, and does not compromise system security;
- Each user has the duty to:
 - (1) respect the privacy and confidentiality of other users,
 - (2) respect the legal copyrights and licenses of programs, software and data,
 - (3) protect data from unauthorized use or disclosure,
 - (4) respect the integrity of computer system,
 - (5) safeguard their accounts and passwords, and change passwords only in accordance with guidelines for valid passwords,
 - (6) abide by generally accepted rules of network etiquette, including being polite and using only appropriate language (abusive language, vulgarities and swear words are not appropriate),
 - (7) report any observations of attempted security violations, and/or violations of this policy, to the appropriate teacher, administrator or the Network Coordinator, and under no circumstance should the user demonstrate the problem to anyone other than the District official or employee being notified;
- Only those users with written permission from the principal or Network Coordinator may access the District's system from off-site (e.g. from home); and
- Any user identified as a security risk or having a history of violations of District computer use guidelines may be denied access to the District's network.

Section 22.9 Prohibited Activity & Uses

- The following is a list of prohibited activities, and violation of any of these prohibitions may result in discipline or other appropriate penalty, including suspension or revocation of a user's access to the system:
- Infringing on any copyrights or other intellectual property rights, including copying, installing, receiving, transmitting or making available any copyrighted software on the District's computer network;
- Using the network to receive, transmit or make available messages that are racist, sexist, abusive or harassing to others;
- Using another person's account or password;
- Attempting to read, delete, forge, copy or modify the e-mail of other system users;
- Interfering with the ability of other system users to send and/or receive e-mail;
- Engaging in vandalism (any malicious attempt to harm or destroy computer system equipment, software or the data, and includes but is not limited to creating and/or placing a computer virus on the network);
- Using the network to send anonymous messages or files;
- Using the network to receive, transmit or make available to others a message that is inconsistent with the District's code of conduct;
- Revealing the personal address, telephone number or other personal information of oneself or another person;
- Using the network for sending and/or receiving personal messages;
- Intentionally disrupting network traffic or crashing the network and connected systems;
- Installing personal software or using personal disks on the District's computers and/or network without the permission of the appropriate District official or employee;
- Using District computer resources for commercial or financial gain or fraud;
- Stealing data, equipment or intellectual property;

- Gaining or seeking to gain unauthorized access to any files, resources or computer or phone systems, or vandalizing the data of another user;
- Using the network while access privileges are suspended or revoked;
- Using the network in a fashion inconsistent with directions from teachers and other staff and from generally accepted network etiquette;
- Transmitting any material in violation of any federal, state and/or local law or regulation, including but not limited to materials protected by copyright, threatening or obscene material, or material protected by trade secret; and/or
- Participating in chat rooms.

Section 22.10 Penalties For Violation

Any user of the system who violates any provision of this policy shall be subject to a penalty consisting of disciplinary action, suspension and/or revocation of computer access privileges, or a combination thereof. In addition to the penalties referred to in paragraph (A) of this section, any information pertaining to or implicating illegal activity will be reported to the proper authorities.

Section 22.11 Website & Webpages

The District website and web pages are intended to support the District's educational mission, provide the community with information about the District and its schools, provide students and the community with support for learning, serve as a channel for feedback from students, families, and the community.

Websites and webpages operated by or on behalf of the District shall be considered District publications over which the District maintains full editorial control. The Network Coordinator will be responsible for overseeing District websites and webpages throughout the District.

The Superintendent or his/her designee shall approve or deny proposed websites and/or webpages based upon certain criteria in the policy

Persons seeking to publish a webpage on the District's website must make application to the Network Coordinator, which is subject to the approval of the Superintendent.