

Selma City Schools

District Technology Policy

Cheating and Plagiarism:

Students are expected to complete all tests and assignments honestly and will not collaborate in dishonest actions. Students will not give or accept answers or assignments unless directed to by the teacher. If a student is found to be cheating, the following will occur as a result of the first and subsequent violations:

- **1st Violation:**
The student's teacher will assign a zero grade on the test or assignment and will call the student's parent or legal guardian. The teacher shall notify the counselor and may refer the student to the principal. Upon referral the principal may place the student on probation in that class for the remainder of the course. The principal may suspend the student and may refer the student to the Executive Committee depending on the severity of the infraction. If a student is placed on class probation, a letter will be sent by the principal to the student's parent(s) or legal guardian informing them of the probation or suspension.
- **2nd Violation:**
If the violation recurs in the same class, the teacher will refer the matter to the principal. The principal will confer with the student. The principal may refer the matter to the Executive Committee for further action, which may include but not be limited to removal from the class, assignment of a failing grade, and reassignment to a supervised study area. A letter will be sent by the principal to the student's parent(s) or legal guardian informing them of the decision.

USE OF DISTRICT TECHNOLOGY

4.8

4.8.1 INTRODUCTION

The primary purpose of the Selma City Schools electronic communications network (SCSNET) and technologies which attach to it is to support and enhance learning and teaching that prepares students for success in an information society. These technologies include all computer hardware, software, and network infrastructure owned or operated by Selma City Schools including its internal network, portals, and/or online resources. Use of the system is defined as obtaining access to any SELMA CITY SCHOOLS technology, software, or services regardless of the technical device, and regardless of whether or not the device is owned or operated by the district. Students, staff, and guests in Selma City Schools who are provided with access to networks (including the

Internet), SCSNET, and other technologies by the District shall be governed by the following policy.

The Internet is a network of networks connecting millions of computer users all over the world. This network enables worldwide connection to e-mail, discussion groups, databases, software, file storage and other information resources, such as libraries and museums. Selma City Schools may provide network access to promote educational excellence in Selma City Schools schools by facilitating resource sharing, innovation, and communication. Selma City Schools firmly believes that the valuable information and interaction available on networks far outweigh the possibility that users may procure material that is not consistent with the educational goals of Selma City Schools. The use of SCSNET is a privilege, not a right, which may be revoked at any time for inappropriate behavior.

Users have no expectation of privacy in their use of SCSNET. SELMA CITY SCHOOLS has the right to access, review, copy, delete, or disclose, as allowed by law, any digitally recorded information stored in, or passed through SCSNET, regardless of the initial intentions of the user. SELMA CITY SCHOOLS has the right and responsibility to monitor the use of SCSNET by its users including tracking of internet, network, hardware, and software use. Employees should be aware that any digitally recorded information, even that of personal nature, can be subject to disclosure under the Illinois Freedom of Information Act. Users assume responsibility for understanding the policy and guidelines as a condition of using the network. Staff members are accountable to teach and use the network responsibly. Use of the network that is inconsistent with this policy may result in loss of access as well as other disciplinary or legal action. Any use of SCSNET during or after the school day by any student, staff member, or guest that disrupts educational process or goals of the institution is prohibited.

4.8.2 PHILOSOPHY

1. **RISK:** It is impossible to control all materials on the network. Sites accessible via SCSNET, particularly networks not under District control, might contain material that is illegal, defamatory, obscene, inaccurate or controversial. With global access to computers and people, there is a risk that students may access material that might not be considered to be of educational value in the context of the school setting. No technology is guaranteed to be 100% error free or dependable. The District makes no warranties of any kind for the service it is providing. The District is not liable or responsible for: 1) any information that may be lost, damaged or unavailable due to technical or other difficulties; 2) the accuracy or suitability of any information that is retrieved through technology; 3) breaches of confidentiality; or 4) defamatory material.
2. **USERS RESPONSIBLE:** Students and staff should use District technology in a responsible, efficient, ethical, and legal manner in accordance with the Selma City Schools mission. Network users, like traditional library users, are responsible for their actions in accessing available resources. The user is responsible for making sure any information received does not contain pornographic or indecent material, inappropriate information, inappropriate language, or files that are potentially dangerous to the integrity of the hardware/software on school premises. The user is not permitted to install any software

that may be used to circumvent network or computer security or to violate any of these policies or break any law.

4.8.3 ACCEPTABLE USE:

All users of the SCSNET must comply with the District's Acceptable Use Policy (AUP), as amended periodically.

SCSNET access may be used to improve learning and teaching consistent with the educational mission of Selma City Schools. District207 expects legal, ethical, and efficient use of the network. These policies apply equally to all District technology including, but not limited to: network services, hardware, software, and other related services currently deployed or to be deployed in the future.

1. **ACCESS:** Selma City Schools may issue accounts to provide access to resources. The use of the SCSNET is a part of the curriculum and not a public forum for general use. Incidental personal use of Selma City Schools technologies should be minimized.
2. **PRIVILEGE:** Use of a personal SCSNET account, once issued, is a privilege, not a right.
3. **VOLUNTARY:** Use of a personal SCSNET account is voluntary on the part of the student or teacher.
4. **SUBJECT TO SYSTEM ADMINISTRATION:** All SCSNET account usage is subject to examination or investigation as needed without prior notification or consent of the user. All users of the SCSNET should recognize that mail use, storage capacity or evening/night/weekend access might be limited for technical reasons. Network administrators may review files and communications to maintain system integrity and to ensure that users including students and staff members are using the system responsibly and according to this policy. Users should not expect that e-mail, data or files stored or transmitted across SCSNET will be private. Employees should be aware that any digitally recorded information, even that of a personal nature, and/or documented use of SCSNET may be inspected and could be subject to public disclosure under the Illinois Freedom of Information Act. All users of SCSNET are guaranteed no level of privacy for any digital information stored or passed through SCSNET. The content of any digitally recorded information might be cause for disciplinary or legal proceedings of students, staff, or guests.
5. **RETENTION POLICY:** The District may retain all digital information, including all e-mail correspondence, indefinitely. This does not guarantee the storage or integrity of all digitally recorded information.

4.8.4 INAPPROPRIATE USE:

Inappropriate use includes, but is not limited to, those uses that violate the law, are inconsistent with Selma City Schools's educational mission, disrupt the educational process, interfere with an employee's performance or work responsibility, that are not in accord with this policy, or that hamper the integrity or security of SCSNET or any external networks to which SCSNET are connected. No type of computing device can be used by anyone, including students, staff, or guests, in any manner that disrupts the educational environment or violates the rights of others, including

using the device to take photographs in locker rooms or bathrooms, cheat, unlawful purposes, bully, harass, or otherwise violate staff or student conduct rules. Prohibited conduct also specifically includes, without limitation, creating, sending, sharing, viewing, receiving, or possessing an indecent visual depiction of oneself or another person through the use of an electronic computing device, mobile or otherwise. Any use of a mobile computing device on school grounds during or after the school day by any student, staff member, or guest that disrupts educational process, goals of the institution, or violates the acceptable use policy is prohibited.

The use of personal electronic devices that attach to the District's secure network is only permitted in the following instances:

- The Technology Department must pre-approve any device before an attempt is made to attach it to the network. Approval will be based on the following requirements:
 - Is the device needed for an educational purpose that cannot be provided with District equipment?
 - Can the device be properly inspected by technology for worms/viruses, hacker software and software or files that in any way violate federal or state law or other provisions of these policies.

The device must be provided to the Technology Department at least one week prior to the planned use so that it can be evaluated. Users cannot attach certain classes of devices by their nature to the network. These include switches, hubs, routers and wireless access points. This regulation applies to any device that connects to the network, including but not limited to cellular telephone, video recording device, personal digital assistant (PDA), electronic paging device, portable gaming system, digital audio or video system, cellular phone, or any other tethered or mobile electronic computing device.

The use of any electronic device to record and/or transmit audio and/or images will not be allowed unless it is part of the curriculum supervised by a teacher or otherwise approved by the Administration. Other devices that do not require a network connection may be governed in other District policies. These include but are not limited to: cell phones, IM (Instant Messaging) devices, text messaging devices, and calculators with advanced communications functions. In addition, any devices for taking pictures and videos or recording audio whether it be stand alone, on a phone, mobile computing device, or wireless, require advanced approval before they can be used.

Users of SCSNET may record after school events as long as they are following this and other District policies with regard to permissions from their students, and if necessary the student's family, they do not need to have approval to record images, video or sound.

1. **COMMERCIAL USE:** Use for non-school sponsored private or commercial, income-generating, financial gain or "for-profit" activities or product advertisement or solicitation purposes or fraud is prohibited.
2. **HARASSMENT:** Harassment, threatening, intimidating, bullying, or demeaning an individual, or group of individuals because of sex, color, race, religion, disability, national origin, or sexual orientation is prohibited.

3. **PROFANITY OR OBSCENITY:** Users are not allowed to access, retrieve, or view obscene, profane, or indecent materials. "Indecent Materials" are those materials which, in context depict, or describe sexual activities or organs in terms patently offensive, as measured by contemporary community standards. "Obscene materials" are those materials which, taken as a whole, appeal to the prurient interest in sex, which portray sexual conduct in a patently offensive way in which, taken as a whole, do not have any serious literary, artistic, political, or scientific value. Use of profanity or obscenity is prohibited, and all users shall use language appropriate for school situations.
4. **OFFENSIVE OR INFLAMMATORY SPEECH:** Users must respect the rights of others, both in the local community and the network at large. Sharing personal information or personal attacks are an unacceptable use of SCSNET. If a user is the victim of an inappropriate communication, the incident shall be brought to the attention of a teacher or system administrator.
5. **VANDALISM/MISCHIEF:** Vandalism and mischief are prohibited. Vandalism is defined to include any attempt to harm or destroy data of another user, on the network or on any networks that are connected to SCSNET or physical damage to District technology. This includes, but is not limited to, the deliberate creation and/or propagation of computer viruses. Mischief includes interference with the work of other users and is prohibited. Any action that disrupts or interferes with the ability of the SCSNET to carry out its intended function may be considered mischief.
6. **USER ID VIOLATIONS:** Once an account is issued to a user, that user is responsible for all actions taken while using that account. Sharing an account with another person, or disclosing another individual's password, is prohibited. Concealing or misrepresenting one's identity while using SCSNET is prohibited. Every user is responsible for all inappropriate uses of the user's account by any other person. All users must exercise extreme caution with their passwords. Passwords must be secure (at least seven characters, one character that is not a letter or number, no simple words or names, nothing easily guessed). Passwords that use two words separated by a non-alphanumeric character are good i.e. Cub\$anto. Logging on, or attempting to log on, in the name or account of another person or entity is prohibited. If a user suspects that any account on the SCSNET has been compromised it is their responsibility to immediately contact the network manager.
7. **ELECTRONIC MAIL VIOLATIONS:** Forgery of electronic mail messages is prohibited. Reading, deleting, copying, or modifying the electronic mail of other users is prohibited. Sending E-mail that is unsolicited junk, rumor, harassment, obscene, or chain letters is prohibited. E-mail that is used to promote a cause for profit or charity must be approved by a building or district administrator. The use of mass mailing should be minimized, and approval for mass messages may be required by a building or district administrator.
8. **FILE/DATA VIOLATIONS:** Users are not allowed to access, retrieve, view, or disseminate any material in violation of any federal or state laws or regulation or Selma City Schools policy or rules. This includes, but is not limited to: improper use of copyrighted material; improper use of files or information on SCSNET to commit fraud, or with the intent to commit fraud; improper use of passwords or access codes; or disclosing the full name, home address, or phone number of any district employee, student, or user. All users of SCSNET are responsible for protecting personal records held in an electronic format. All users of SCSNET are not allowed to download, copy, print or otherwise store or possess any data which violates federal or state copyright laws or these guidelines.

9. **NON-ACADEMIC USE:** District technology is a valuable, scarce resource. It is not to be used for non-academic purposes such as game playing unless approved by the Superintendent or the Superintendent's designee. Unauthorized intentional downloads to a single computer, network drive or external media of movies or video files; MP3s; shareware; freeware; pirated software; or other .exe or application files (unless a part of the curriculum) are not allowed. It is not to be used to access pornography or obscene materials under any conditions, nor can it be used to forward chain letters.
10. **SYSTEM INTERFERENCE/ALTERATION:** Attempts to exceed, evade or change resource quotas that may be established are prohibited. Quotas are limits on local hard drive storage space or network time or storage space which are designed to allow all users an equitable opportunity to access resources. Causing network congestion through mass consumption of system resources is prohibited. Any attempt to circumvent security on desktop machines or mobile computing devices is prohibited. Transfer of software to or from SCSNET is not allowed without authorization by the Chief Technology Officer or designee.
11. **ELECTRONIC COMMUNICATION:** Any use as a forum for communicating by e-mail or other medium with other school users or outside parties to solicit, proselytize, advocate, advertise, or communicate the views of an individual or non-school sponsored organization; to solicit membership in or support of any non-school sponsored organization; or to raise funds for any non-school sponsored purpose, whether profit or non-profit are all prohibited uses of SELMA CITY SCHOOLS net. No employee shall knowingly provide school e-mail addresses to outside parties whose intent is to communicate with school employees, students, and/or their families for non-school purposes. Any communication that represents personal views as those of the school system or any school unit or that could be misinterpreted as such is not allowed. Employees who are uncertain as to whether particular activities are acceptable should seek further guidance from their immediate supervisor.
12. **SOFTWARE LICENSING:** The district must own and maintain a license, or have on record evidence of acceptable use, for any software installed on a school owned computer. Users of district owned computing devices may not install any software, licensed or otherwise, without permission from the Chief Technology Officer or designee.
13. **WEBSITES AND SOCIAL NETWORKS:** Users of SCSNET also agree to follow the Website guidelines outlined in Maine Township High School Selma City Schools Board Policy 6511 regarding websites and social networks.
14. **EDUCATIONAL PROCESS:** Any action that takes place on SCSNET, or external networks, that may disrupt the educational process, including use that is reasonably foreseeable to result in disruption, or interfere with the rights of others at any time, either during the school days or after school hours, is prohibited.

4.8.5 VIOLATION OF LAW:

Transmission of any material in violation of any international, U.S., or state law is prohibited. This includes, but is not limited to: copyrighted material; music; software; threatening, harassing or obscene material; or material protected by trade secret. Any attempt to break the law while using Selma City Schools facilities may result in prosecution or litigation against the offender. If such

an event should occur, Selma City Schools will fully cooperate to the extent permitted by law with the authorities to provide any information necessary in connection with prosecution.

4.8.6 CONSEQUENCES OF POLICY VIOLATION:

A user's network access privileges may be interrupted or terminated for any violation or attempted violation of this policy.

A user's network privileges may be interrupted or suspended by a technology department staff member, administrator, or the Chief Technology Officer while a suspected violation is being investigated and while determination of any appropriate discipline is in progress. During such an investigation and determination, alternative opportunities for the user to complete assignments will be made available where appropriate and reasonably possible. Before suspension or termination of network privileges, the user will be advised of the suspected violation and given an opportunity to respond as part of the discipline procedures (which are part of Board Policy and are contained in the Discipline Procedures booklet).

Violators will also be subject to disciplinary measures, such as suspension from school or expulsion for students or appropriate penalties for staff in accordance with the Discipline Procedures, Collective Bargaining Agreement between the Board of Education and the Maine Teachers' Association, or staff handbooks. Guests that violate the acceptable use policy may be barred from using SCSNET or from being present on school grounds.

4.8.7 SECURITY:

When using any part of SCSNET a user agrees to maintain security and to the District enforcing security in the following ways:

- **HIGH PRIORITY:** Security on any computer system is a high priority, especially when the system involves many users, provides access to personal data, or can be used to view, edit, or delete student records.
- **REPORTING SECURITY PROBLEMS:** If a user identifies a security problem on the network it is expected that he or she will notify the District Director of Technology or a designee. The user must not share the security problem with other users.
- **USER RESPONSIBILITIES:** The user is accountable for reasonably responsible behavior to ensure security. The user must follow network guidelines in the selection of an appropriate password. The user must protect the confidentiality of their password.
- **SCSNET NET FILTERING AND MONITORING:** Selma City Schools has the right to filter any content from SCSNET that is deemed inappropriate by the administration. Selma City Schools may monitor any SCSNET users, and the information gathered may become public under the *Illinois Freedom of Information Act*.
- **SECURITY RISKS DENIED ACCESS:** Any user identified as a security risk or having a history of violations with other computer systems may be denied access to SELMA CITY SCHOOLS net through Selma City Schools facilities. It is the intent of Selma City Schools to prohibit access to such persons.

4.8.8 DISCLAIMER:

Selma City Schools makes no warranties of any kind, whether expressed or implied, for the network facilities it is providing. Selma City Schools will not be responsible for any damages suffered by users. This includes loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions caused by its own negligence or user errors or omissions. Selma City Schools is not responsible for phone/credit card bills or any other charges incurred by users. Use of any information obtained via the network is at the user's risk. Selma City Schools specifically denies any responsibility for the accuracy or quality of information obtained through its network facilities. The district is not responsible for any user's intentional or unintentional access of material through SCSNET which may be obscene, indecent, or of an appropriate nature.

Adopted: ????