POLICY

SOMERSET COUNTY
BOARD OF EDUCATION

Date Submitted: July 21, 1998 **Date Reviewed:** March 21, 2000 December 16, 2008 June 21, 2016 October 16, 2018	**Number:** **500-14**
Subject:	**Date Approved:** August 18, 1998 January 20, 2009 July 19, 2016 October 16, 2018 **Date Revised:** March 21, 2000 December 16, 2008 June 21, 2016 October 16, 2018 **Date Effective:** July 1, 2002 January 20, 2009, July 19, 2016 October 16, 2018

1. PURPOSE:
To establish guidelines for acceptable use of Somerset County Public School information technology systems, resources, the Internet and email.

A. Definitions

1) System Administrators – The person(s) responsible for running, managing, and maintaining a technology system or service.
2) Information Technology – Systems and resources
3) Electronic Communication Systems – Electronic communication systems include, email, instant messaging, online discussions, video communications or any method or service that communicates using digital technology.
4) SCPS Affiliated technology services – Services provided by a third party such as Microsoft or Google through an SCPS administered program or license.
5) Personally Identifiable Information - Information that can be used to identify, contact or locate a person and includes but is not limited to: name, family member's names, addresses, phone numbers, Social Security numbers, or student ID numbers.
6) HIPPA – The Health Insurance Portability and Accountability Act is designed to protect the confidentiality and security of healthcare information.
7) CIPA – The Children's Internet Protection Act was enacted by congress to ensure that schools put Internet safety policies and protective measures in place to protect children from obscene or harmful content over the Internet.

8) COPPA – The Children's Online Privacy Protection Act regulates online services and their privacy protection requirements and consent requirements for children under 13 years of age.
9) FERPA – The Family Educational Rights and Privacy Act is a Federal law which protects the privacy of student educational records.

2. ACCEPTABLE USE:

A. Introduction

The staff and students of Somerset County Public Schools are provided with access to information technology systems, resources, and electronic communication systems for educational purposes, including interacting with and participating in our global society. Information Technology accounts provided by SCPS or through SCPS affiliated technology services are to be used in a responsible, effective and lawful manner for school related purposes.

The Superintendent, Administrators, and the System Administrators of technology services are delegated the authority to determine appropriate use and may request to deny, revoke, suspend or close any user account at any time based upon his/her determination of inappropriate use by the account holder or user.

B. Legal Context

All existing federal, state, and local laws as well as the regulations and policies of Somerset County Public Schools are applicable to this AUP, including laws and regulations that are specific to technology and laws that may apply generally to personal conduct.

C. Supervision and Monitoring

Somerset County Public Schools has the right to monitor, track, log, access and report on all aspects of its Information Technology systems and their use. Users will have no expectation of privacy or ownership with regard to their use of any SCPS technology resource even if they are used for personal reasons. The Information Technology resources, electronic communications and information accessible via the SCPS network are the property of Somerset County Public Schools.

Random audits of Internet activity and Information Technology systems and their use may be run on a regular basis and any suspicious or inappropriate access will be reported to appropriate administrators or supervisors. In addition, any illegal activities will be reported to the appropriate agencies. SCPS may access media brought onto its premises, at district events, or connected to the district's technology resources to ensure compliance with this policy and other district policies.

D. Filtering

In compliance with the Children's Internet Protection Act, SCPS will deploy technology to block or filter Internet access to prevent users from accessing Internet content that is considered inappropriate. Any attempt to circumvent or disable content filtering is strictly prohibited.

E. Cyber Safety

Somerset County Public Schools will make every possible effort to assure the safety of our students as they access the Internet through our technology resources during the school day. Cyber safety lessons are included in the students' technology and media curriculums. These lessons teach students about respecting other peoples' rights online, keeping their own identity private, internet safety, and copyright compliance.

F. Copyright & Intellectual Property Rights

SCPS staff and students are expected to comply with the procedures outlined in SCPS Policy #500-35 in the use of publications, software, video and audio recordings, and information found on the Internet to protect the authors of these works from infringement upon their legal rights. These procedures have been developed to adhere to federal copyright laws (see www.copyright.gov) and to the SCPS policy on the Evaluation and Selection of Instructional Materials Policy #500-19.

G. User Responsibilities

Staff and students are expected to use technology resources in a responsible, ethical and legal manner for school-related purposes in accordance with this policy, and all referenced laws, policies and regulations. Staff members are responsible for providing appropriate adult supervision of student technology use.

1. The possession, use, transmission or importing of offensive, obscene, libelous, disruptive, or inflammatory language, pictures, or other material on any computer, electronic device or any information technology system within SCPS or within SCPS affiliated online services is prohibited.
2. The violation of confidentiality or privacy laws is prohibited including the intentional disclosure, use, or distribution of another individual's personally identifiable information.
3. Any attempt to circumvent technology security measures is strictly prohibited. This includes making connections to the Internet through means other than those provided by SCPS.
4. Real time communication systems and collaborative online tools such as instant messaging, Wikis, threaded discussions, online chats and video conferencing may only be used by students under the direct supervision of a teacher for school-related activities with permission from an administrator. Staff members using these tools with students are responsible for monitoring discussions, content, and interactions for appropriate educational use.
5. The violation of copyright laws is prohibited. This includes sharing, installing, recording or distribution of copyrighted software, audio and video media. This also includes installing or copying SCPS licensed software or applications to non-SCPS owned equipment unless specified in the licensing agreement.
6. Intentionally obtaining, using, modifying or destroying content, passwords, or data belonging to other users without their consent is strictly prohibited.
7. Sharing passwords with others is prohibited. All users are responsible for any actions that occur under their account.

8. Attempting security breaches or disruptions of any electronic communications system is prohibited. This includes, but is not limited to tampering with the security of SCPS owned computers, network equipment, services or files.
9. Attempting to access systems or areas of Information Technology Systems for which a user has not already been granted permissions is prohibited.
10. Users may not download, install or use any unauthorized software or apps on SCPS technology resources without permission from System Administrators.
11. Knowingly performing actions that will disrupt the operation of any SCPS Information Technology System is prohibited. This includes disrupting another user's ability to use those resources.
12. Knowingly spreading computer viruses, worms, malware, spyware, Trojans, or any other computer software that is malicious in nature is strictly prohibited.
13. Use of the SCPS technology resources to threaten or harass others is prohibited. Any harassment or inappropriate message encountered should not be responded to and should be reported to an appropriate staff member.
14. End user installation of wiring, wired network equipment, wireless network equipment or any extension, retransmission, or interception of the SCPS network is prohibited.
15. Using SCPS technology resources for personal commercial purposes or attempting to profit from the use of SCPS technology resources is prohibited.
16. Use of websites or online services which violate the provisions of student privacy laws, such as COPPA and FERPA and are prohibited.

H. Consequences for Violations:

The use of SCPS technology resources is a privilege, not a right. Inappropriate, unauthorized, or illegal use or any violation of the conditions and rules in this policy may result in the individual's access being revoked. Misuse will also subject the student/staff to disciplinary action under individual school building policies and/or Somerset County Board of Education policies. In addition, any illegal activities will be reported to the appropriate agencies. Any costs incurred due to individual negligence or misuse of SCPS technology, including damaged, lost or stolen items, will be the financial responsibility of the negligent individual(s).

I. Website and Web-based Content Standards:

The primary purpose of operating websites is for SCPS students and staff to share information about curriculum, instruction, authorized activities and resources that enhances teaching, learning and communication.

All subject matter permitted on SCPS websites and any links to other web sites must relate to school business, curriculum and instruction, research that is related to the school system, supervised classroom projects and/or course work, and school related activities or organizations.

All information developed for a SCPS website must be free of spelling and grammatical errors not contain language and graphic art and/or photographs that are inappropriate, focus on violence, rude behavior, racism, blasphemy, and/or any and all provocative anti-social conduct.

J. Electronic Communications

Electronic communication accounts provided by SCPS or through SCPS affiliated electronic communication services are to be used in a responsible, effective and lawful manner for school related purposes. All electronic communications created, received, or stored on SCPS electronic communications systems are the sole property of SCPS and not the author, recipient, or user.

Unacceptable uses of SCPS electronic communications include, but are not limited to:

1. Receiving, displaying, storing, or transmitting threatening or sexually-explicit images, messages, or cartoons as well as epithets or slurs based upon race, ethnic or national origin, gender, religious affiliation, disability, or sexual orientation and harassing, offensive, discriminatory, or defamatory communications or images without an educational purpose is prohibited.
2. Sending or responding to lengthy private messages is prohibited.
3. Using SCPS electronic communications systems to send political messages is prohibited.
4. Engaging in any activity that is illegal under Local, State or Federal law in conjunction with the usage of SCPS electronic communication systems is prohibited.
5. Disclosure or transmission of confidential information, Personally Identifiable Information, or HIPPA protected information of themselves or others is prohibited.
6. Sending electronic communications using another person's account or credentials is prohibited.
7. Interference or disruption of services, including distribution of unsolicited advertising, mass sending of non-school related unsolicited email, and/or propagation of malware is prohibited.
8. Disguising or attempting to disguise your identity when sending or using electronic communications systems is prohibited.
9. Users should not forward or retransmit electronic communications or attachments without acquiring permissions from the sender.
10. The storage of confidential, SCPS, or State owned information on mobile devices or removable media is prohibited.

There should be no expectation of privacy in anything created, stored, sent or received through SCPS provided electronic communication systems except where required by law. SCPS reserves the right to access, intercept, inspect, record, and disclose any electronic communications on SCPS electronic communications systems or SCPS affiliated electronic communications services unless prohibited by law or privilege. Messages sent and received are subject to the Freedom and Information Act and Maryland public disclosure laws. All emails sent and received using SCPS email systems are archived and kept for a minimum of five years.

K. Disclaimer:

SCPS liability for use of its information systems and technology resources is limited to:

1. Notification to users that all provisions of the AUP are subordinate to local, state and federal statute; and
2. While users are prohibited from using electronic communication for advertising, commercial purposes, religious activities, and any non-governmental-related fund raising

or public relations activities, such as solicitation for religious purposes, lobbying for political purposes, or soliciting votes, SCPS does not condone and is not responsible for these and any and all activities in which users might engage.