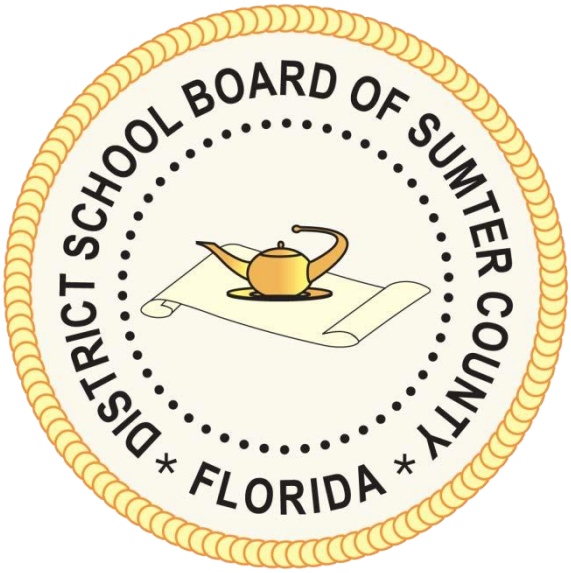

NETWORK & INSTRUCTIONAL TECHNOLOGY POLICIES AND PROCEDURES

SUMTER DISTRICT SCHOOLS

2680 West CR 476
Bushnell, Florida 33513

Updated 4/30/2021

TABLE OF CONTENTS

SUMTER COUNTY SCHOOL BOARD NETWORK & INSTRUCTIONAL TECHNOLOGY POLICIES AND PROCEDURES

Sumter County School Board (SCSB) Network and Instructional Technology Policies and Procedures exist in addition to all other legally binding documents to guide the conduct of the Sumter County School Board users. It is not intended to replace in part, or in whole, pertinent Florida or federal laws. Such laws include the Computer Crimes Act, Chapter 815 of the Florida Statues; the Public Records Law; Chapter 119 of the Florida Statutes; the Digital Millennium Copyright Act; the Computer Fraud and Abuse Act of 1986; the Computer Abuse Amendments Act of 1994; or obscenity and child pornography laws. Additionally, activities related to Management Information Services (MIS)/Data Processing processes are governed by other requirements and are covered by *Management Information Services: Data Processing Section Operations Manual.*

All users agree to comply with the SCSB Information Technology Policies and Procedures with applicable state and federal laws dealing with appropriate, responsible and ethical use of information technology. It is not the responsibility of the IT Department to ensure user compliance with this technology policy. It is the responsibility of the user to be aware of the existing policies and to adhere to their guidelines. Non-compliance is a serious breach of the Sumter County School Board's standards and may result in legal and/or disciplinary action for all users, employees and students.

These policies are applicable to all SCSB technology resources and are global in scope. It may become necessary for individual departments and/or schools to define in more detail the limitations on their internal computing resources by further refining the policies stated here. No department and/or school may override the guidelines and restrictions contained within this technology policy.

ACCESS TO POLICY

Sumter County School Board (SCSB) Information Technology Policies and Procedures shall be made available on the SCSB website, http://www.sumter.k12.fl.us and/or internal sites readily available to all users. The specific Acceptable Use Policy (7540.04) can be found as part of the Sumter District School Board Policies online and in printed form as well as a component of the SCSB Information Technology Policies and Procedures. The *Employee Technology Handbook* is updated yearly and includes the information of the SCSB Information Technology Policies and Procedures in a concise and user friendly format. This handbook will be available to all users in both print and online access.

All account requests must be accompanied by the *Staff Network Account Request (PS-130)* form.

OWNERSHIP AND USE OF INFORMATION TECHNOLOGY RESOURCES

The information technology resources provided and maintained by Network Services are intended for SCSB related purposes including the support of the SCSB mission, its administrative and instructional functions and activities within the user community. Appropriate use of computing resources includes respecting the privacy of other users and their accounts, using only those resources you are authorized to use, respecting the finite capacity of these resources so as not to limit their accessibility by others and abstinence from using any of these resources for personal gain or commercial use not related to SCSB business. Unauthorized and/or inappropriate use of these resources is prohibited and may result in disciplinary and/or legal action. Unauthorized or fraudulent use of SCSB telecommunications resources can result in felony prosecution as provided for in Florida Statutes. Resource areas are defined as follows:

Technology Equipment

Technology equipment may include but is not limited to workstations, laptops, mobile communication devices, tablets, servers and network devices such as routers, patch panels, switches and wireless access points. SCSB may require users of computing equipment to limit or refrain from specific uses of that equipment if their activities are destructive or interfere with SCSB technology operations or resources. No unauthorized user may connect to any SCSB network resource that provides access to the internal network of the district. This includes personal use computers or devices, equipment owned by sales representatives, consultants, and/or other visiting professionals. Only SCSB technology equipment is authorized for use on the SCSB network. An SCSB computer may be loaned upon request with 48 hours' notice to sales representatives, consultants, trainers or others as needed for network access. The district network manager has the authority to approve specific contracted services to access the network with their own equipment when such connection can be done securely and safely. Examples of possible connection consideration would include auditors with the Auditor General Office, installation engineers with specific approved applications and similar services.

Software

For the purpose of this policy and procedure manual, the term software will include not only applications installed directly on individual computers but also applications installed on any technological device OR that is accessed by said devices from cloud based resources.

Software owned by the SCSB will be installed on computers and devices set up for the end users by an SCSB technology support technician or a person designated to install software at a school site. All software installed on SCSB computers must be properly licensed and authorized.

Prior to purchase, the technology support team should be informed of the requested purchase, upon which the software will be reviewed as to compatibility with existing systems and whether the application meets the security expectations. Unless a full operational pilot has been used to test the application, our ability to ascertain the actual usability, will be limited.

GUIDELINES FOR THE USE OF SCSB TECHNOLOGY RESOURCES

It is a general policy that the network/Internet will be used in a responsible, efficient, ethical, and legal manner in accordance with the mission of the Sumter County School Board. Failure to adhere to policies and guidelines may result in legal and/or disciplinary action.

Technology Acceptable Use (SCSB Board Policy 8.62)

The data network system of the District is available for use by employees and students of the District in order to provide them with equal access to the computing resources which serve public education. The data network system is an electronic highway that connects thousands of computers all over the world and millions of individual subscribers. All personnel having authorization to use the network will have access to a variety of information sources. The District's technological resources are components of the data network system. This policy is in effect whether the district owned resource is connected to the district network or in use outside the network.

I. The use of these technology resources is a privilege, not a right.

II. No expectation of privacy or confidentiality in the content of electronic communications including, but not limited to, computer files, electronic messaging, facsimile or other transmissions sent, received through or stored on the communication resources of the Sumter District Schools should be expected by users. Such information is subject to review, monitoring and archiving. The District reserves the right to remove them and report any violation of rules to school and/or District administration and/or law enforcement. For the safety and security of students, District supported electronic communications for students will be monitored and filtered.

III. Access to material on the worldwide interconnected network, does not provide for the use of the same selection procedures as the School District follows in regard to other instructional materials, such as textbooks. Similar to broadcast and other current event media, the material available is vast and ever changing. With such access, comes the potential availability of material that may be harmful to minors or not be considered to be of educational value in the context of the school setting. Specifically, the District supports those which will enhance the research and inquiry of the learner with directed guidance from faculty and staff. At each school, each student's access to use the network will be under the teacher's direction and monitored as a regular instructional activity.

IV. The District will maintain technology protection measures to limit student's access to prohibited material. While the District uses Internet content filters, any filtering

of information should not be considered all inclusive. The District cannot prevent the possibility that some users may access material that is not consistent with the educational mission, goals and policies of the District. This is particularly possible since access to the Internet may be obtained at sites other than school or on devices outside the authority of the school. The Sumter District Schools reserves the right to limit the content of material students access due to legitimate pedagogical, safety and system integrity concerns.

V. At each school and facility owned or operated by the District, notices shall be conspicuously posted that state the following:

> "Users of the data network system of the Sumter County School District are responsible for their activity on the network. The School District has developed a technology resources acceptable use policy. All users of the network are bound by that policy. Any violation of the policy may result in the suspension of access privileges or other disciplinary action, including student expulsion and employee dismissal."

VI. The use of the network and technological tools shall be consistent with the mission, goals, policies, and priorities of the District. Successful participation in the network requires that its users regard it as a shared resource and that members conduct themselves in a responsible, ethical and legal manner while using the network.

Any use of the network or technological tools for illegal, inappropriate or obscene purposes, or in support of such activities, will not be tolerated. Examples of unacceptable uses of the network or technological tools include, but are not limited to:

A. Violating the conditions of the Education Code dealing with student's rights to privacy;

B. Using, transmitting or accessing profane, obscene, lewd/indecent (which includes what is commonly referred to as sexting) or other materials harmful to minors;

C. Copying commercial software or other content in violation of copyright law or other copyright protected material;

D. Using the network or technological tools for financial gain or for any commercial or illegal activity;

E. Using the network or technological tools for the advancement or disparagement of any particular candidate or political party;

F. Taking any actions that affect the ability of the District to retrieve or retain a record of any use of the computer equipment or data network system, including but not limited to, adding or modifying the existing software without specific permission; creating, uploading and/or intentionally accessing computer viruses or material blocked by the District's technology protection measures; intentional damage to technological equipment or

any other action for the purpose of limiting the usability of the network or technological tools.

G. Taking any actions that affect other students' ability to use the technological resources, including but not limited to, vandalism or "hacking".

H. Transmitting student identifying information over the data network system, except as part of the approved educational program as permitted by law; and

I. Other actions that are not in accordance with the *Code of Ethics* and *Principles of Professional Conduct of the Education Professional of Florida* for staff and *The Code of Student Conduct* for students.

VII. Schools and Departments in the Sumter School District may have additional guidelines for appropriate use. These policies will be developed and enforced in consort with this District policy.

VIII. Schools are required to educate their students about appropriate online behaviors including but not limited to interactions with other individuals through communication methods or social networking. Instruction will include cyber bullying awareness and response.

IX. The District recognizes the use of social media for communication and e-learning; however, only those networks sponsored by the District may be used for classroom instruction or school sponsored activities without the approval of the Superintendent or his designee.

X. Failure to adhere to this policy may result in suspending or revoking the offender's privilege of access to the network and other disciplinary action up to and including, termination of the employee or expulsion in the case of a student, and possible criminal prosecution if applicable. Any possible illegal acts discovered by students or employees shall be reported to the appropriate legal authority.

XI. Any student shall be exempt from instruction on accessing the data network upon request in writing from the parents, as defined by Florida Statutes, to the principal. The request for exemption shall expire at the end of each school year. It shall be the responsibility of the parent to renew the request yearly.

STATUTORY AUTHORITY: **1001.41, 1001.42, F.S.**

LAW(S) IMPLEMENTED: **1000.21, 1001.43, F.S.**

HISTORY: **ADOPTED: 11/16/2004**
REVISION DATE(S): 3/7/2006, 8/7/2007, 4/3/12, 9/4/2012
FORMERLY: 2.52

Network Security and Safety Guidelines

In order to protect the resources and privacy of all using district resources, every teacher and administrator should remember the following:

1. Acceptable uses of the network are activities which support learning and teaching. Network users are encouraged to develop uses which meet their needs and which take advantage of the network's functions: email, conferences, access to databases, and access to the Internet that are safe and supportable and meet the expectations of the Acceptable Use and Internet Safety Policy.
2. It is the responsibility of the faculty member who grants access to SCSB facilities and/or resources to insure that students are aware of the provisions of the SCSB acceptable use policies and guidelines, and of any rules, procedures, or courtesies for the outside network they are accessing.
3. It is the responsibility of the faculty member to always supervise students when they are accessing the network.
4. Whenever possible place the computers in central locations in the classroom or media center, where the screens are highly visible.
5. Discuss the Acceptable Use and Internet Safety Policy and other guidelines that promote educationally relevant and personal safe uses of the Internet and technology.
6. Since filtering isn't foolproof, users are still responsible for appropriate use.
7. Access should be limited only to educational sites.
8. Do not reveal your personal information or that of any other person such as name, address, phone number).
9. While teachers and staff have the ability to access most personal web based email systems, the use should be minimal. These are to only be used for personal correspondence. For the purpose of archiving, all communications related to the operations of the school district must process through the managed email systems of the district. In the situation a personal account is used, it is imperative that a copy is also sent to the users district account so it will be archived.
10. Student electronic communications are to only occur through district provided means. The school is required to be in compliance with the *Children's Internet Protection* and the *Protecting Children in the 21st Century Acts.* District provided communication systems will provide tools to protect the safety and security of minors when using.

Access to Technology Resources

Users will be granted appropriate access to the technology resources necessary in conducting SCSB business related to their job function. Normal operation and maintenance

of computing resources requires: backups and caching of data communications, logging of resource activity, remotely accessing files and computer processes, monitoring of general usage patterns, as well as other activities necessary in providing service to the user. SCSB may monitor activity and/or accounts of individuals without notice.

User Accounts

Appropriate persons will be authorized to access the SCSB network. Access to the administrative systems are requested, managed, reviewed and approved through a separate process through the Management Information Services / Data Processing Department.

Staff access to the SCSB Network will be initiated through the submission of a PS-130 form to the Information Technology Department. General network accounts will provide access to:

1. Membership into a staff user Active Directory Security Group and related shared resources
2. Computer login credentials
3. An email account
4. Access to Office 365 One Drive for storage of documents
5. Internet Access

Additional accesses managed through Active Directory or other managed authentication systems can be authorized through the request of the appropriate administrator(s). Access may include but not limited to: the administrative systems, school website management, Local Instructional Improvement Systems, instructional applications, etc. Access to these resources will be authorized if such operation is a part of, or directly related to, the workload of the school or administrative unit. It is the responsibility of the individual's supervisor to ensure proper training and use of any computer programs or data files.

When employment with the SCSB terminates, or duties are changed so that the specific access to computer equipment or data files is no longer required or a transfer to another school or department is made, the user account must either be disabled or altered to reflect the change in the individual's position, departmental or school affiliation. In the case of termination/resignation, the Human Resources Department will inform the network manager or other designated technical support personnel of the effective date. Access will be disabled effective 12:00 midnight of the effective date unless due to unique circumstances earlier action is required.

It is the responsibility of the individual's supervisor to inform network services when changes of location or job duties at the school site change that impact their specific access requirements.

Students, volunteers and non-school staff are not to be provided access to controlled SCSB data resources. Non-permanent substitutes are typically not approved for network accounts or email addresses. In situations of long-term substitutes or other unique situations, the school principal or department head may petition the Senior Director of Curriculum for a waiver.

Passwords

Upon approval of access to the SCSB staff network, the school's or department's technology contact will be provided with the login information to provide to the new user. The technology contact will be available to assist the new user with any questions related to use or appropriate use. This initial password will be set to require the new user to change the initial password upon their first login. This password is to be kept secure and not provided to others under any circumstance.

All network passwords must:

1) Be a minimum of 12 characters
2) Passwords must be complex including a minimum of three of the following type of characters:
    a. Upper case letters,
    b. Lower case letters,
    c. Numbers and/or
    d. Symbols.
3) Passwords must be changed every 90 days.
4) Passwords cannot be repeated until after ten unique passwords have been used.
5) Accounts will lock upon three unsuccessful attempts.
6) After 15 minutes of inactivity, district managed workstations will lock and require the reentry of the user's network password in order to continue using the computer

Passwords to individual applications not managed by the District's Active Directory may be different. If the application does not support password complexity enforcement, the standards of network password security will be expected from staff end users.

Disclosure of Passwords

It is a violation for any person to disclose their individual staff network password to any other person.

In unique situations, the password of non-active directory managed applications may need to be provided to a member of technical services for problem resolution. Such passwords must be changed upon resolution. Thus, it is the responsibility of each employee to maintain the confidentiality of password(s). Under no circumstances shall any password be posted or kept in a place that is accessible.

In the situation of web based applications/sites that are not managed by the Sumter Network & Instructional Technology, where data may be posted in accordance with the district's Web Publishing Policy, an administrative account login must be made available for administrative oversight and policy enforcement.

Access to these accounts and their passwords to any unauthorized personnel are prohibited. It is the responsibility of the account owner to immediately change their password upon the suspicion of any compromised password or unauthorized access as well as informing the

Network Manager or administrative staff as identified in the Data Loss Prevention or Incident Response Plan.

Network Management and Security

In the information age in which we live, management of network resources and the security of the Sumter County School's network are fundamental to the pursuit of the SCSB goals of academic excellence and serving the needs of Sumter County Schools. While school board policy 7540.04 identifies the acceptable use and Internet Safety expectations, Network resources, accepted network behavior and their associated policies are further defined as follows:

Bandwidth

Bandwidth, or the transmission capacity, of our network hardware is a finite resource all electronic information on our network must share. This information can be referred to as network traffic. SCSB reserves the right to use tools, including access restrictions to govern these priorities based on the relative importance to the overall mission of the district of different applications, users, and groups in conjunction with available resources.

Hacking

Hacking is the interference with or unauthorized access to any computer or computer network. This may or may not reflect malicious intent. Specific examples of 'hacking' include but are not limited to:

1) Any attempt to gain root or system administrator privileges on any SCSB network device or service, without permission;
2) Any attempt to gain unauthorized access to files, devices or accounts;
3) Any attempt to do anything that would result in the interruption of any service to SCSB users;
4) Any attempted use of password cracking software including wireless encryption protocols;
5) Circumventing SCSB approved firewalls or technology protection measures, such as content filters and security devices;
6) Specific software attacks, including denial of service attacks;
7) Any attempt to access or change system files, without permission;
8) Any unauthorized attempt to store user files outside their predefined areas;
9) Installation or attempted use of SUID (Set User ID) programs of any type, without permission. SUID's are often used to allow users on a computer system to run programs with temporarily elevated privileges in order to perform a specific task;

10) Any attempt to do the above mentioned items through the SCSB network, even if the attempt is aimed outside the network;
11) Use or access of applications or services for the purpose of accessing materials for the purpose of violating copyright or to access materials not permitted by school rules, civil or criminal law;
12) Transmitting protected data outside of permitted uses;
13) Port scanning and/or sniffing is not permitted within the SCSB Network except for approved system management by network technology technical services personnel;
14) The operation of any unapproved DNS or DHCP services within access of devices on SCSB property for the purpose of intercepting/hijacking network device traffic;

Hacking may compromise system availability, data integrity or both. SCSB will, to the fullest extent allowed by law, seek legal and/or disciplinary action against any individual(s), organization(s) and/or company(s) that directly or indirectly utilizes our network (or causes it to be used) for any practice that is considered to be hacking .

Network Infrastructure and Communications Closets

The network infrastructure or hardware includes but is not limited to switches, hubs, routers, patch panels, fiber optic cables and interfaces and other network cabling. Only those individuals authorized through Technology Services, Management Information Services or specific communication personnel of the facilities department will be allowed access to these communications resources.

In addition, Technology Services must authorize all networking equipment in use and connected to the network prior to being physically attached to that network. Unless specifically exempted, technology services staff will manage all network equipment. Any unauthorized equipment of any kind found attached to the network will be disconnected immediately without notice and may be confiscated by technology services.

Network Address Assignment and Dynamic Host Configuration Protocol (DHCP)

Each device attached to a network must have a unique address associated with it. The assignment and accurate maintenance of these addresses is key to a healthy, functioning network. Management of these functions is solely the responsibility of technology services. DHCP is a readily available method by which address assignment can be automated. No unauthorized use of DHCP will be permitted and may be considered within the realm of “hacking.” Any unauthorized device acting as a DHCP server will be disconnected immediately without prior notification to the owner and may be confiscated by technology services.

Domain Name Registration

The Network Technology Services s is the only authorized agent for the Sumter County School Board who may register a domain name/host name to any network device or Internet service before its installation on the SCSB network or registered with an Internet domain registrar. All requests for device domain names/host names and network addresses must go through network technology services and it will be their responsibility to verify will review requests making certain requested domain names are appropriate, consistent with the mission of the SCSB and in compliance with standard naming conventions.

Wireless Networks

The design, operation and management of the wireless network is the responsibility of the Information Technology Services. Wireless equipment includes but is not limited to wireless transceivers or Access Points directly connected to the wired network and wireless antennas which amplify radio frequency signals. Any tampering with any of these devices will result in appropriate disciplinary action. As with other unauthorized network infrastructure, any unauthorized wireless device found connected to the wired network will be disconnected immediately without notification to the owner and may be confiscated. If other wireless devices in use cause interference with the network, Network Technology Services will work with the school or department operating the device to try and find an alternative solution.
All approved wireless access devices are required to encrypt data transmitted.

The district will operate three parallel wireless networks. The “District Network” is intended for access only by district owned devices. The “BYOD” network is specifically to support Internet only access for personal devices and the “Bring Your Own Device” (BYOD) initiatives. The “Guest” network will not have access to resources or data within the Sumter network and will be ported directly to the Internet. Such access will require authentication with network credentials. Any use of devices attached to the guest network must be in accordance with the SCSB Acceptable Use and Internet Safety Policy. Additionally, Network Technology Services reserves the right to authorize devices and collect information including MAC Addresses and Internet access history while using the SCSB Internet gateway.

Anti Virus / Anti Malware / SPAM Control/ Patch Management

The District utilizes various enterprise level tools to protect the network and data from malicious intent. End users are not permitted to circumvent or disable these protection tools. These tools include:

1. Desktop Security Protection with automatic update services
2. Enterprise Gateway Security Protection with automatic update services
3. Managed gateway firewall software/hardware based
4. Intrusion Prevention
5. Electronic Mail SPAM Controls with automatic update services

6. Network equipment management including firmware updating services
7. Microsoft Update Management implemented
8. Technology Protection Device for Content Filtering

MOBILE DEVICE SECURITY

Policy Statement

Due to the increased risk of loss or theft, every member of the SCSB community who utilizes devices that are designed to be portable or easily transportable, is responsible for the District data stored, processed and/or transmitted via that computer or device, and for following the security requirements set forth in this policy and in the Acceptable Use Policy and Internet Safety Policy.

The purpose of this policy is to comply with federal regulations governing privacy and security of information, and to protect Confidential Data in the event of the theft or loss of such mobile devices. The Family Educational Rights and Privacy Act of 1974 (FERPA) is a federal guarantee of the privacy of educational records for student and their parents. Additionally, other privacy and security laws, such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and Gramm-Leach-Bliley/Financial Services Modernization Act of 1999 (GLBA), may also apply.

Definition

Mobile devices will include any device that is designed to be portable or easily transportable and capable of storing district data. This may include but not be limited to: laptop computers, tablet computing devices, smart phones (i.e. Blackberry, iPhone, Android, Windows Phone, etc.), removable media (i.e. jump/flash drives, CD-R , DVD-RW, SD and similar memory devices, diskettes, etc.), external hard drives, and other personal digital assistant devices (PDA).

Confidential Information

Information protected by statutes, regulations, SCSB policies or contractual language. Managers may also designate data as Confidential. Any disclosure of Confidential Data must be authorized by the Sumter County Superintendent of Schools or his/her designee. By way of illustration only, some examples of Confidential Data include:

1) Medical records,
2) Student records and other non-public student data,
3) Social Security Numbers,
4) Student Psychological Reports,
5) Personnel and/or payroll or records,

6) Individualized Education Plans,
7) Credit card or bank account numbers,
8) Facility or technology security procedures or processes,
9) Any other information specifically exempt from public information by SCSB policy 3.50 and
10) Any data identified by government regulation to be treated as confidential, or sealed by order of a court of competent jurisdiction.

ELECTRONIC MAIL

The Sumter Schools' E-mail system is provided for the specific purpose of supporting its educational mission and the related business operations. It is important to understand that every email sent from the Sumter Schools' E-mail system reflects on the district as a whole. Keep emails professional.

LIMITED personal use of the e-mail accounts has been permitted but users must strictly adhere to the overall standards as set forth in the acceptable use policy.

While limited personal use has been permitted, the school e-mail account **is not a replacement for a personal email account**. Free or inexpensive web-based e-mail accounts are provided by several online companies including *Yahoo, Google, and Microsoft*.

Florida has relatively open public information laws and no email messages, including personal e-mails, should be considered private and may possibly be released as public information. Also, the E-Mail system is the property of the School District of Sumter County. All E-Mail messages written using the system are also the property of the District. Treat electronic communications the same as written hard copy communications with regard to propriety and openness. The District reserves the right to review all electronic correspondence that use District systems and facilities.

·In order to meet federal and state law, the Sumter school district archives electronic communications using its system.

Distribution lists within the district address book should never be used to send personal emails.

·No personal technology use, including e-mail, should interfere with performing ones job function.

·One should not use their district account to register or list as their contact email for non-school related situations. (e.g. ebay, retail stores, online retailers, contest registrations, etc).

Specific guidelines for the appropriate use of electronic mail:

The use of proper English and grammar is expected in all correspondence using the Sumter electronic mail system. The school system promotes academic achievement and a high respect for intellect. All correspondence sent from the school district should reflect such values.

The sending of mass emails is only appropriate in extremely limited circumstances and only in circumstances that promote the operational and educational goals of the district. Under no circumstance should emails be sent for personal gain, including for the purpose of promoting or selling services or property or promoting non-school events/activities.

One should not email forwarded personal messages to those that you have not discussed their desire to receive them from you, first.

Users should be aware that picture, sound and video files may be quite large and occupy valuable technology resources which may impair the primary uses of the technological systems. **The forwarding of chain letter emails are never appropriate.**

The district uses technological tools to limit the number of unsolicited junk emails, called "SPAM," the accounts receive. While this system cannot stop all unsolicited e-mail, it is relatively effective. . If you feel a legitimate email has been stopped, please inform network services as soon as possible. While much junk mail is sent with no interaction by the recipient, evidence shows that one is far more likely to receive many more such emails if:

Their email address has been used to register for contests or other marketing techniques on websites,

Their email address is highly prominent on websites, or

The user sends or receives forwarded messages which have many recipients listed.

Additionally, malicious computer programs and not protecting the security of one's password are two means that increase the issuance of SPAM. Such programs or having access to one's email account can allow the sending of SPAM emails to others.

Do not open attachments or follow links from senders you do not know or from whom you are not expecting an email. This is a common method of sending computer viruses, malware and attempts to gain personal information.

WEB PUBLISHING

The Sumter County School Board provides Web hosting services to all SCSB schools and departments in the district. The use of web pages and web sites must be in support of educational and professional activities that are consistent with the educational goals and policies of the Sumter County School Board. This policy applies to all associated web content hosted by the SCSB including but not limited to, all web pages supported on the SCSB servers,

whether created by school, departments, staff, or students. Web pages are public documents inviting the outside world to the individual schools, departments and the school district, while at the same time linking students and staff to outside sources of information. All web pages hosted on the SCSB servers are the property of the Sumter County School Board.

Responsibilities

Webmaster responsibilities are designated by the principal or department supervisor. Upon notification network services will assign rights to the individual(s) designated. Network Services will provide assistance to webmasters as to web management, copyright and security requirements upon request by the principal or department supervisor.

All Sumter County School web pages will reside on SCSB network servers unless designated service providers are selected and approved by Network Services and the SCSB.

Design and Development Guidelines

1. While schools have latitude on their design, the authoring tools and processes must adhere to the underlying server technologies offered by Network Services. If a school would like Network Services to investigate additional server technologies, it can be requested, but under the realization this would be considered an enhancement requiring testing and implementation that cannot be expected to be accomplished quickly.
2. School webmasters are encouraged to review the needs of their school and select publication of information that is relevant and helpful to the school or department's mission.
3. It is imperative that web sites are kept up-to-date and old materials are removed when no longer relevant. Since search engine "crawlers" may index files available within websites whether there are active links or not, so it is important to remove files when they are no longer part of the website.
4. Websites must be developed in accordance with current copyright laws as per SCSB policy.
5. Student pictures may be posted but in accordance with the stipulations of directory information and not violate the restrictions of the Family Educational Rights and Privacy Act of 1974 (FERPA). Students' parents are informed of their rights when enrolled or at the beginning of the year. It is important to verify that a student's parent has NOT noticed the SCSB that they do not wish directory information to be released on their child prior to including their picture or name on the website. This information is documented within the student record in the TERMS Student Information System.

DATA LOSS PREVENTION: NETWORK AND INSTRUCTIONAL TECHNOLOGY

Policy Statement

Protection of data stored on the network resources is of a paramount importance to the school district. The purpose of this policy is to comply with federal regulations governing privacy and security of information, and to protect Confidential Data from theft or loss. The Family Educational Rights and Privacy Act of 1974 (FERPA) is a federal guarantee of the privacy of educational records for student and their parents. Additionally, other privacy and security laws, such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and GrammLeach-Bliley/Financial Services Modernization Act of 1999 (GLBA), may also apply. See the section on Mobile device security.

The SCSB technological services follow the *National Institute of Standards and Technology* Cybersecurity Framework to reduce cyber risks to the District's technological infrastructure and data. Through considerations within the five functions (Know, Prevent, Detect, Respond and Recover), the District organizes its security processes to meet expectations and needs.

Backup Strategies

All protected data will be backed up on a regular basis, of no less than once a week. Backups may be in the form of virtual server snapshots/images, individual file backups and/or SQL database backups. Copies will be stored in secured environments outside of the building housing the original data.

Physical Security

All district level servers and storage arrays will be housed in secured areas. The data centers will remain locked and only accessible by authorized personnel. In the event of other personnel needing to access the space, the individual will be accompanied by an authorized individual. The Network Operation/ Data Center will be protected with security to include burglary, excessive heat and fire.

The resources housed in the MIS Data Center and Network Operations/Data Center are protected through battery backups and auxiliary power generators. The Network Operations/Data Center also is equipped with redundant cooling systems.

All drive arrays for protected data will be RAID 5 or greater configurations for data protection.

Confidential Information

Information protected by statutes, regulations, SCSB policies or contractual language.

Managers may also designate data as Confidential. Any disclosure of Confidential Data must be authorized by the Sumter County Superintendent of Schools or his/her designee. By way of illustration only, some examples of Confidential Data include:

1) Medical records,
2) Student records and other non-public student data,
3) Social Security Numbers,
4) Student Psychological Reports,
5) Personnel and/or payroll or records,
6) Individualized Education Plans,
7) Credit card or bank account numbers,
8) Facility or technology security procedures or processes,
9) Any other information specifically exempt from public information by SCSB policy 3.50 and
10) Any data identified by government regulation to be treated as confidential, or sealed by order of a court of competent jurisdiction.

Server and Storage Classification

While the protection of all resources is important, it is also important to identify data storage that contains confidential information and develop more rigorous processes to protect the data.

Due to the confidential and mission critical information housed within the district's Student Information, Human Resources and Finance/Business Management Systems; these systems are classified as sensitive data. Data Loss procedures within these systems will be under the direct management of Management Information Services / Data Processing.

Within the resources supported under Network and Instructional Technology, the department will review the data servers and classify those that would contain confidential information and create special access procedures for access. Access shall only be provided with the expressed consent of the specified data owners.

PROTECTED SHARES

Special shared storage resources are provided to departments with the need to share classified information between authorized users within their department. Protected shares are hidden from other network users. Creation and access to a protected share is governed by the individual department's administrator.

ADMINISTRATIVE DATA BASES

These data include Student, Human Resources, Payroll and Financial information and currently maintained on systems managed outside the scope of network security and data support. Access to this information is granted based on a request by the administrator of the applicable department.

These systems are backed up nightly and the backup tapes are stored in an offsite location. Weekly backups are to be maintained for seven days and month end backups are to be saved for two months.

SECURITY INCIDENT RESPONSE: NETWORK AND INSTRUCTIONAL TECHNOLOGY

The following operating procedure is followed when security events occur, incidents involving network and Instructional Technology systems or requests for information that involve user activity. Additionally, this includes alerts or advisories that impact personnel using IT systems connected to the SCSB network environment.

Incident severity classification

Level 1 Incident – Security incident involving Unrestricted Data that is not protected by law, contract or whose disclosure would cause no harm to the school district or to individuals. A Level 1 incident would include temporary abnormalities to networking systems that do not show any security compromises.

- Report incident to Network Services with as much detail as possible
- If incident is related to a user account, the user must change their password immediately.
- Network Services will review the incident, verify the level of incident and make proper repairs and corrections to the system as necessary.
- In the case of temporary abnormalities that might affect the end user and the level of classroom management needed, an alert should be sent to the users (i.e. a temporary failure of Internet filtering, virus protection, etc.)
- Network Services will document as necessary.

Level 2 Incident – Security incident involving breeches to control and protection systems or hacking that affects network performance and/or Internet reputation (e.g. circumvention of

logging, bypassing or exploiting a weakness in filtering, or other networking system that does not involve confidential information.

- Report incident to Network Services with as much detail as possible.
- Network Services will review the incident, verify the level of incident and make proper repairs and corrections to the system as necessary.
- All such breeches are to be reported to the Coordinator of Media & Technology.
- Network Services will investigate and in the case of student behavior, will inform the principal or designee of the details of the technology offense for possible disciplinary action and adjustments in classroom technology management.

Level 3 Incident – Security incident involving Restricted (non-personal) Data whose unauthorized access, modification or loss could affect the school district adversely

- Report incident to Network Services with as much detail as possible
- Network Services will review the incident, verify the level of incident and make proper repairs and corrections to the system as necessary.
- Level 3 Incidents will be reported to the Coordinator of Media & Technology.
- Network Services will document as necessary including a notation any data that could not be repaired or that had to be recreated.

Level 4 Incident – Security Incident involving Confidential Information

- Report incident to Network Services with as much detail as possible
- Network Services will make the initial review the incident and if emergency corrections are necessary, will complete as quickly as possible. If related to any network accounts, the user passwords are to be changed immediately.
- The Coordinator or Media & Technology, Senior Director of Curriculum and the supervisor of any Department directly affected will be informed of the security incident.
- Network Services will further access the information that was possibly compromised, and make the proper repairs and corrections.
- Senior management will be consulted on any specific need to report the security incident as might be required by law.
- Network Services will report on the incident and recommendations of changes to correct or improve security systems and processes to reduce the possibility of future incidents.

Investigations

Student

Investigations of student technology related may be requested by the school principal or assistant principal or a district administrator.

Such investigations may include providing access for the school administrator to gain access to restricted locations or network technical staff reviewing network resources.

Network technical staff can assist school personnel in understanding the severity of a technological offense to assist them in an appropriate response.

Staff

Administrative staff may request assistance of the network technical staff to identify information related to the work activities of their staff members in the event they suspect a use of technology that may affect their work or the responsible actions in running their department or school site. Additionally, as per Board Rule 6.27, "all employees shall be responsible for reporting misconduct by School Board employees that affects the health, safety or welfare of a student;" requires network staff to report misconduct they observe though their normal work duties.

Official staff investigations will be initiated by a senior director or the superintendent. Network technical staff will follow the administrator's directives. Network technical staff may provide professional interpretation of the findings.

Alerts and Advisories

Network Technical Staff will strive to stay informed of security alerts and advisories from organizations such as:

1) National Institute of Standards and Technology (NIST) http://csrc.nist.gov/
2) Microsoft Security Response Center (MSRC) http://www.microsoft.com/security/msrc/default.aspx
3) CERT Center, Carnegie Mellon University http://www.cert.org/
4) SysAdmin, Audit, Network, Security (SANS) http://www.sans.org/ 5) Kaspersky Labs https://my.kaspersky.com/