



## **Information Technology Policies and Procedures**

**Suwannee County School District**

**September 23, 2014**

# TABLE OF CONTENTS

TABLE OF CONTENTS .....	1
1.0 OVERVIEW .....	2
2.0 PURPOSE .....	2
3.0 SCOPE .....	2
4.0 ACCEPTABLE USE POLICY .....	2
4.1 GENERAL USE AND OWNERSHIP .....	2
4.2 SECURITY 4.2.1 PASSWORDS, ACCOUNTS, AND ANTIVIRUS .....	3
4.2.2 <i>Network Security and Administrator Rights</i> .....	3
4.3 SENSITIVE AND CONFIDENTIAL INFORMATION .....	3
4.3.1 <i>Definition and Protection</i> .....	3
4.3.2 <i>Access and End User Support</i> .....	4
4.4 GUEST AND VENDOR ACCESS .....	4
4.5 USER LAPTOP POLICY .....	4
4.6 REVOCATION OF PRIVILEGES .....	6
5.0 UNACCEPTABLE USE .....	6
5.1 UNACCEPTABLE USE: SYSTEM AND NETWORK ACTIVITIES .....	6
5.2 UNACCEPTABLE USE: EMAIL AND COMMUNICATIONS ACTIVITIES .....	7
6.0 NETWORK ADMINISTRATOR RESPONSIBILITIES .....	8
7.0 SECURITY INCIDENTS .....	8
7.1 DEFINITION .....	8
7.2 RESPONSE .....	9
7.3 MONITORING .....	9
7.3.1 <i>Devices and Applications</i> .....	9
7.3.2 <i>Files and Correspondence</i> .....	9
8.0 DATA LOSS PREVENTION .....	10
9.0 PURCHASING .....	10
10.0 TECHNOLOGY COMMITTEE .....	10
11.0 ENFORCEMENT .....	11
12.0 REVISIONS .....	11
APPENDIX A .....	12
APPENDIX B .....	13
APPENDIX C .....	14
APPENDIX D .....	16

## 1.0 Overview

The IT Department's intention for publishing Policies and Procedures is not to impose restrictions that are contrary to Suwannee County School District's established mission of providing users with the best tools possible to educate every student. Rather the IT Department is committed to protecting Suwannee County School District's users from illegal or damaging actions by individuals, either knowingly or unknowingly. Network related systems, including but not limited to computer equipment, software, operating systems, storage media, mobile devices, network accounts providing electronic mail and or resources, WWW browsing, and FTP, are the property of Suwannee County School District. These systems are to be used for educational and school business-related purposes with the intent of serving the interests of the students, teachers, and other staff members of Suwannee County Schools District. Maintaining a network requires proper planning, organization, monitoring, and effective security. A team effort involving the participation and support of every Suwannee County School District employee and affiliate is required to meet and exceed the standards set forth by Florida State Law, Federal Law, and the Suwannee County School District's Board and administrators. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

## 2.0 Purpose

The purpose of this policy is to outline the acceptable use of the network-related systems within the Suwannee County School District. These rules are in place to protect the students, staff, and the Suwannee County School District. Inappropriate use, improper planning, and disregard of these procedures exposes Suwannee County School District to risks including compromise of network systems and services, possible damage to the network, and legal issues.

## 3.0 Scope

This policy applies to students, employees, contractors, consultants, temporaries, authorized guests, and other workers at Suwannee County School District, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Suwannee County School District to include all future purchases.

## 4.0 Acceptable Use Policy

### 4.1 General Use and Ownership

- Users should be aware that the data they create on the network remains the property of Suwannee County School District. Users should have no expectations of expressed or implied privacy.
- Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Network/Internet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.
- Using the Suwannee County School District network is a privilege. As with all privileges, it is the responsibility of the guest user to use this service appropriately and in compliance with all school board policies and procedures, Florida state law, and Federal laws.
- The use of excessive bandwidth and reproduction of copyrighted materials is strictly forbidden and will result in the termination of network services.
- The Suwannee County School District assumes no responsibility for costs associated with loss or damage to devices not owned by Suwannee County School District while on the network.
- For security and network maintenance purposes, the IT Department may monitor equipment, systems, and network traffic at any time.

- The Suwannee County School District's IT Department reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

## 4.2 Security

### 4.2.1 Passwords, Accounts, and Antivirus

- Users, which includes employees, students, and guests of Suwannee County School District, will be granted access to the network after they have signed the appropriate Network Usage Agreements forms (see Appendix A, Appendix C, and Appendix D).
- Users must keep passwords secure and are not share accounts. Authorized users are responsible for the security of their passwords and accounts.
- Users shall not leave computer unattended while logged on.
- Users of Windows based computer's will be required to change their passwords every 45 days as prompted automatically by Windows Active Directory.
- Users needing password resets for various programs must contact the IT Department. Every attempt will be made to identify the user by positive identification. This method may include sight/voice reconciliation, a predetermined security question, or other questions as determined by the Director of Technology.
- All computers used by students, employees, or guests that are connected to the Suwannee County School's network, whether owned by the user or Suwannee County School District, shall be continually executing virus-scanning software with a current virus database.
- Users must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

### 4.2.2 Network Security and Administrator Rights

- Administrative passwords for the network, servers, computers, wireless access points, and other electronic devices are to be kept strictly confidential and known only by IT staff members that need them to perform their duties. Distributing passwords of any kind is strictly forbidden.
- Wireless access points will be secured with a security mechanism to be determined by the IT Director. The wireless security code will be entered into authorized devices by the IT staff only. Any attempt to obtain and/or distribute this code is strictly forbidden.
- Users using Suwannee County School District devices will not be granted Administrative Rights to those devices unless they submit a written request to the IT Department proving that they have a legitimate need for such rights. The IT Director and/or IT staff will determine if there is another alternative before granting such rights.

## 4.3 Sensitive and Confidential Information

### 4.3.1 Definition and Protection

When handling sensitive and confidential information, precautions must be taken to prevent unauthorized access to the information. Staff members may not disclose sensitive information to persons not authorized to receive it. This includes non-public information such as Social Security Numbers, credit card numbers, bank account numbers, health information, or other confidential student and user data.

All users who have access to or may have access to personally identifiable student and user records shall adhere to all standards included in the Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), Suwannee County School Board Policies and Procedures, and all other applicable State and Federal laws and regulations, as they relate to the release of such information.

Below are the guidelines that must be followed where applicable:

- Encrypt data.
- Password protect data.
- Physically protect devices that can be easily moved such as PDA and Laptops that are used to access sensitive data.
- Avoid creating files that use social security numbers as identifiers. Use employee numbers and/or student local identification number instead.
- Never download or copy sensitive data to your home computer
- Never store un-encrypted data on a portable device
- Protect printed sensitive data. Store sensitive data in locked desk, drawer or cabinet. Do not leave unattended sensitive data on copier, FAX, or printer. Shred sensitive data that need to be disposed.

#### 4.3.2 Access and End User Support

Sensitive data access is restricted to only those personnel who need to perform their job duties. Access restrictions to such data are maintained by the IT Department in conjunction with the Finance Department, the Human Resources Department, the Superintendent of Suwannee County School District, and the School Board. Accesses to sensitive information are only granted at the request of an administrator with an accompanying and verifiable need.

Reviews of accesses and privileges are conducted regularly and monitored to ensure compliance with all School Board Policies as well as State and Federal Laws and regulations.

#### 4.4 Guest and Vendor Access

- Guest and Vendor access will not be granted to any Suwannee County School District network or network device without a signed and approved vendor contract or a Guest Access Agreement Form (Appendix D).
- Using the Suwannee County School District network is a privilege. As with all privileges, it is the responsibility of the guest user to use this service appropriately and in compliance with all school board policies and procedures, Florida state law, and Federal laws.
- The use of excessive bandwidth and reproduction of copyrighted materials is strictly forbidden and will result in the termination of network services.
- The Suwannee County School District assumes no responsibility for costs associated with loss or damage to devices not owned by Suwannee County School District while on the network.
- The Suwannee County School District IT staff can provide limited support in aspects of network connectivity and access of network resources.
- Backing up data and ensuring the security of network devices are the sole responsibility of the owner.
- Vendor supplied user ID's, program passwords, guest accounts, and security devices are administrated by the IT Department. This information and these devices are kept secure from general users unless knowledge of them is imperative to the course of their job.

#### 4.5 User Laptop Policy

- Users that are issued laptops by the Suwannee County School District must sign a Laptop Usage Agreement form upon receipt of the laptop (see Appendix B).
- Users will be responsible for the security of the laptop while assigned to them whether on or off campus.
- Users acknowledge that issued laptops are property of Suwannee County School District and shall be returned in their original condition upon request.

- Users assume all risk of injury or harm associated with the use of the laptop off-premises, including but not limited to, physical damage or loss, or personal injury.
- While laptops are being used off campus, the Suwannee County School District has no control over the information accessed through the internet and cannot be held responsible for content viewed.
- Suwannee County School System and its users will not be held liable for claims for damages that may arise from the use of issued laptops while not on school property.

## 4.6 Personal Technology Use

Personal technology refers to computer equipment, software, operating system, storage media, mobile device, or a technology program or device that is the personal property of employees, students, or guests of Suwannee County School District.

- The School District of Suwannee County does not insure personal property of students, staff, teachers or the public brought on school property. Property of this nature that is stolen, damaged or lost is the sole responsibility of the owner. The Suwannee County School District assumes no responsibility for costs associated with loss or damage to devices not owned by Suwannee County School District while on the network. Suwannee County School District assumes no responsibility for the technical support or functionality of personal technology brought on school property.
- With the exception of phones and tablets, no personal devices shall be granted network access by Suwannee County School District. Personal phones and tablets will be authorized for network access at the discretion of the Director of Technology, and such access will be granted as Guest access only and may be revoked at any time.
- The use of personal USB Flash Drives is authorized to employees and students of Suwannee County School District for administrative and educational purposes permitting that such use complies with all policies set by Suwannee County School District.
- Data created on the network through personal technology remains the property of Suwannee County School District. Users should have no expectations of expressed or implied privacy.
- With the exception of authorized devices listed above, under no circumstance shall personal technology in the form of software, programs, applications, hardware, or other computer equipment and peripherals be installed, attached, or otherwise joined to the technology property of the School District of Suwannee County

## 4.7 Donation of Technology

Technology donations to the District in the form of software, programs, applications, hardware, or other computer equipment and peripherals must have prior approval of the Director of Technology before being presented as a donation or gift to Suwannee County School District in accordance with Board Policy 9.021. The following conditions must be met before approval shall be considered:

- All donations of technology must be intended for school educational purposes and for the benefit of students.
- All items must be purchased new within the last six months with receipt or other documented proof of purchase.
- Software must be sealed and/or have no prior installations or registrations.

- Donated items intended for a specific purpose, department, or school must be authorized by respective Principal or District department head. Respective administrator shall agree to assume responsibility for any supplies and/or maintenance of donated technology.
- Donator agrees that the Technology Department does not express or imply any guarantees of current or long-term compatibility among donated technology items and any network related system of the School District. Donator also agrees that donations of technology become the permanent property of the School District and shall be under the full control of the School Board.

## 4.8 Revocation of privileges

Privileges and accesses to all Suwannee County School District network devices, software, email, and information systems will be revised or revoked as necessary in the event of the following

- Transfer of employee
- Resignation of employee
- Retirement of employee
- Termination of employee
- Termination of vendor contract.
- Termination of consulting contract
- In the event of an investigation of employee, vendor, or consultant where revision or revocation of privileges and access is necessary.

## 5.0 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host, if that host is disrupting production services).

- Under no circumstances is an employee, student, or authorized guest of Suwannee County School District authorized to engage in any activity that is illegal under local, state, federal or international law, while utilizing Suwannee County School-owned resources, to include the network and Internet.
- Users shall not access, download, store, send, or display text, images, movies, or sounds that contain pornography, obscenity, or language that offends or degrades others.
- Attempts to circumvent or defeat mechanisms put in place by the Suwannee County School District staff to manage the network is strictly forbidden.
- Users shall not attempt to download and/or install services, electronic file sharing mechanisms, games, software, tools, or any executable file including but not limited to the following file types: .exe, .bat, .cmd, .zip, .msi, and .rar.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

### 5.1 Unacceptable Use: System and Network Activities

The following activities are strictly prohibited, with no exceptions:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Suwannee County School District.

- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Suwannee County School District or the end user does not have an active license is strictly prohibited.
- Exporting software, technical information, encryption software or technology.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- Using a Suwannee County School District computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- Making fraudulent offers of products, items, or services originating from any Suwannee County School District account.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the user is not an intended recipient or logging into a server or account that the user is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Port scanning or security scanning unless prior notification and approval is received beforehand.
- Executing any form of network monitoring unless prior notification and approval is received beforehand.
- Circumventing user authentication or security of any host, network or account.
- Interfering with or denying service to any user other than the user's host (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the network/Internet.
- Providing information about, or lists of, Suwannee County School District's users to parties outside the Suwannee County School District without prior permission from the Superintendent of Schools.

## 5.2 Unacceptable Use: Email and Communications Activities

- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
- Students shall not use social network sites including, but not limited to, myspace.com, facebook.com, chat rooms, etc.
- Students shall not agree to meet with anyone met online.
- Students shall only access the network on equipment intended for student access. The use of faculty-assigned computers is prohibited.
- Students shall not attempt to or obtain any form of confidential information not belonging to that respective student.
- Unauthorized use, or forging, of email header information.
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- Use of unsolicited email originating from within Suwannee County School District's networks or other internet/network service providers on behalf of, or to advertise, any service hosted by Suwannee County School District or connected via Suwannee County School's network.
- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).



## 6.0 Network Administrator Responsibilities

It is the responsibility of the network administrator to follow the guidelines and policies of the Director of Technology, Suwannee County School District, Florida Department of Education, and all State and Federal Laws.

Network Administrators report to the Director of Technology. Regular meetings, as determined by the Directory of Technology, are to be held between the Network Administrators and the Director of Technology in order to maintain close working relationships and openness in day-to-day communications.

Among their other responsibilities, the Network Administrator should use reasonable efforts to:

- Respond to requests for support, information, problem determination and problem resolution.
- Become familiar with all applicable Suwannee County School District IT policies.
- Participate in required Network Administrator training and regular meetings as determined by the Director of Technology.
- Take precautions against theft of or damage to the system components and information.
- Comply with terms of all hardware and software licensing agreements applicable to the system.
- Treat information about, and information stored by, the network users in an appropriate manner and to take precautions protecting the security of the network and the security and confidentiality of the information contained therein.
- Promptly inform the Director and/or Assistant Director of Technology of any computing incidents which clearly compromise network integrity, including but not limited to:
  - Notification by outside institutions or individuals of any incident.
  - Data loss or theft.
  - Inappropriate systems or information access or use
  - Any other breach or violation of IT policies of which they become aware.
- Promptly notify the Director and/or Assistant Director of material changes in network architecture or administration.

Network Administrators, when requested, are expected to cooperate fully with the Director of Technology in any investigation, identification, and resolution of network incidents.

Network Administrators are not responsible for the content of files, images, video or audio clips, electronic communications, and news postings produced by others. The Network Administrator is also not responsible for unauthorized software installed by others. Network Administrators are responsible, however, for notifying the Director of Technology of any observed violations of Suwannee County School District policies, licensing agreements with software manufacturers, or observed violations of local, state, or federal laws regarding these matters.

## 7.0 Security Incidents

### 7.1 Definition

A security incident is any violation of set Policies and Procedures that may or may not result in the following:

- loss of information confidentiality (data theft)
- compromise of information integrity (damage to data or unauthorized modification)
- theft of physical IT asset including computers, storage devices, printers, etc.
- denial of service
- misuse of services, information, or assets
- infection of systems by unauthorized or hostile software

- an attempt at unauthorized access
- unauthorized changes to organizational hardware, software, or configuration
- reports of unusual system behavior etc

## 7.2 Response

If a Network Administrator becomes aware of a security incident, they must provide notification of the incident to the Director of Technology. Upon confirmation, the Director of Technology will notify the user's supervisor (if a Suwannee County School District employee) or School Administrator (if a Suwannee County School District student).

Other steps that may be taken:

- Temporarily suspend or restrict the user's computing privileges during the investigation.  
Reactivation is at the discretion of the Directory of Technology.
- Remove the affected computer device, as appropriate, from the network.

These steps may be taken only after authorization by the Director of Technology unless the situation represents an emergency or immediate threat to network security/integrity. In such case, the Network Administrator must take corrective action and notify the Director of Technology as soon as possible. Actions should be taken in such a way that any impacts to non-offending users are minimized.

## 7.3 Monitoring

### 7.3.1 Devices and Applications

In effort to maintain network security, integrity, and to reduce the risk of Security Incidents the IT Department, at the discretion of the Director of Technology, can and will monitor network activity. These monitoring devices/applications include but are not limited to:

- Firewall logs
- Web Filtering logs
- Network Traffic Monitoring
- Active Directory Monitoring
- Mail Scanner logs
- Database, backup, and usage logs on servers
- Event logs and histories created in individual machines

### 7.3.2 Files and Correspondence

In the course of their duties, it may be necessary for Network Administrators to view files, data or communications that have been stored by users on devices or network file servers. The viewing of such material is permitted only when it is necessary to troubleshoot problems at the request of the user, protect the security and integrity of the Suwannee County School District's network, protect the rights or property of Suwannee County School District or third parties, or to ensure compliance with Suwannee County School District policy or applicable law. Examples include:

- the identification/restoration of lost, damaged or deleted files;

- the identification of a process that is interfering with normal network functions;
- or in more serious circumstances, an investigation of a Security Incident.

In all such cases, the Network Administrator shall take into consideration the confidential nature of files and/or communications that may potentially be reviewed and shall implement the appropriate safeguards to ensure that all local, state and federal privacy laws are complied with. The Director of Technology must be advised of and approve any non-routine monitoring that occurs. Non-routine monitoring includes directed investigations of potential policy and/or security violations. Discovery of such violations in the course of routine monitoring must be reported.

## 8.0 Data Loss Prevention

To prevent data loss from a disaster, the IT Department will follow all disaster policies and guidelines set forth by the Suwannee County School District. In addition, the IT Department will take routine measures to protect and restore critical on-site systems by performing daily, weekly and monthly backups and storing backups in three separate and secure locations. Contacts for information systems off-site include data loss protection plans and disaster recovery plans as a rule before approval.

In the event of immediate threat the IT Department will take the following actions:

- Backups will be performed and stored in all three locations if possible
- Most servers except First Class E-mail will be shut down.
- The generator will be started if needed for power.
- Information will be provided on the Suwannee County School District web site.
- Network closets and battery backups (UPS) should be turned off if unnecessary
- In the event that a Data Center is damaged or destroyed, operations will be re-established at one of the schools or department buildings.

Each school and district office department should take the following steps to protect data and equipment:

- Computers should be turned off and unplugged, if connected to battery backups there should be turned off and unplugged as well.
- Computers should be moved away from windows, off the floor, and covered with plastic if possible.

## 9.0 Purchasing

The IT department is responsible for the seamless integration of any hardware or software into the existing network system and maintaining an inventory of all such items. When considering the purchase of any technology related item, prior approval from the IT Department is required. Procedures to obtain approval for purchase of technology equipment are determined by the Finance Department. A verbal request is not acceptable. In addition, a quote for purchases is not an approval for purchase.

## 10.0 Technology Committee

The Suwannee County School District will maintain a Technology Committee comprised of the IT Director and other IT staff as necessary, District level Administrators, and one administrator and one faculty member from each school.

The Purpose of the Technology Committee is:

- To provide a forum to discuss issues, concerns, and/or interests of the teachers and administrators at each school with the IT Department.
- To assist in promoting the efficient use of technology in schools, including creating standards for the management and application of technology.
- To serve as a resource for Suwannee County Schools in helping all users understand technology in schools and how to use it properly and efficiently.
- Assist in planning for and evaluating classroom technology (such as model classrooms and educational software).

- Assist in planning professional development activities related to technology.
- Assist in other activities as deemed appropriate by the committee in collaboration with the IT Department and Superintendent of Schools.

## **11.0 Enforcement**

Failure to adhere to these policies and guidelines may result in suspension or revocation of the offender's privilege or access to the network and/or other disciplinary or legal action.

## **12.0 Revisions**

The Suwannee County School District reserves the right to change these policies and procedures at any time to ensure the operability and safety of the network and its users.



**Suwannee District Schools IT Department**

**Employee Network Usage Agreement Form**

I have read, understand, and will abide by the provisions and conditions of the Suwannee County School Board Information Technology Policies and Procedures. I understand that any violations of these provisions may result in disciplinary action, the revocation of my access privileges, and/or appropriate legal action. All the guidelines described in the IT Policies and Procedures and the Suwannee County School Board Policies are applicable when I am on the Suwannee County School network.

I further understand that my failure to sign this agreement will result in my access to the Suwannee County Schools Network, Internet, and the e-mail system being completely denied. I also agree to report any known misuse of the network to my immediate supervisor.

**I also understand that this agreement is effective for the duration of my employment with the Suwannee County School System.**

Upon signing this agreement, the employee verifies that she/he has had no employment disciplinary record for on-line technology abuse in her/his present or former workplace. The employee also verifies that she/he has not been found guilty in a United States civil or criminal court for violating any state or federal computer/technology laws. If the employee has been found guilty of violating state or federal computer/technology laws, she/he must attach a separate paper explaining the violations.

**Employee Name (Please Print):** \_\_\_\_\_

**EMPLOYEE SIGNATURE:** \_\_\_\_\_ **DATE:** \_\_\_\_\_



**Suwannee District Schools IT Department**

**Laptop Usage Agreement Form**

Employee Name \_\_\_\_\_

School or Location \_\_\_\_\_

Property Record # of laptop \_\_\_\_\_

Serial Number of laptop \_\_\_\_\_

I acknowledge receipt of the laptop computer assigned to me by the Suwannee District School system for the purpose of removing it from school property for school-related use. I agree I will be solely responsible for the laptop's security and care while it is off school premises and in my personal custody and control. Further, I agree to return it in its original condition when requested.

- I agree to assume all risk of injury or harm associated with the use of this laptop off-premise, including but not limited to, physical damage or loss, or personal injury.
- While off campus the Suwannee County School System has no control over the information accessed through the internet and cannot be held responsible for content viewed.
- Therefore I agree to release Suwannee County School System and its employees from all liability, claims, damages, and causes of action that may arise from my use of this computer while not on school property.

Signature \_\_\_\_\_

Date \_\_\_\_\_





## IT DEPARTMENT STUDENT NETWORK USAGE AGREEMENT

The Suwannee County Schools Network is an electronic network which serves public education in accessing the Internet. The Internet is an "information highway" connecting thousands of computers and millions of individual people all over the world. Students, teachers, and support staff Suwannee County School Network accounts have access to electronic mail (E-Mail) with the ability to communicate with people all over the world. Information, news, and data can also be received from a variety of world-wide sources.

With access to computers and people all over the world comes the availability of some material that may not be considered to be of educational value within the context of the school setting. Efforts have been made to direct participation to education-related materials only. However, on a global network, it is impossible to control all materials. The Suwannee County School Board has established Acceptable Use Guidelines for all users of technology and the Internet in the school system. ***If any user violates any of these guidelines, his/her access to the network will be terminated and appropriate disciplinary and/or legal action will be taken.***

### ACCEPTANCE OF GUIDELINES

As the parent or guardian of this student, I have read the Acceptable Use Guidelines for technology use and Internet use and understand that Internet access via the Suwannee County Technology Network is being provided for educational purposes only. I further understand that it is impossible for the Suwannee County School System to restrict access to all controversial materials, and I will not hold the Suwannee County School System responsible for materials acquired on the Suwannee County Technology Network. ***I also understand that if my child violates any of the rules of the Acceptable Use Guidelines, the Student Code of Conduct, or the Suwannee County School Board Policies/Rules regarding technology or Internet use, appropriate disciplinary/legal action will be taken.***

---

Signature of Parent or Guardian

---

Date

**CHECK THE APPROPRIATE BOXES BELOW, SIGN, AND RETURN FORM TO SCHOOL SITE**

☐ **YES** I have read and understand the Student Network Usage Agreement Form, and understand that this agreement will be in effect until rescinded by me, the undersigned. I DO give my permission for my child to use Suwannee County Schools' technology network to access the internet; **OR**

☐ **NO** I have read and understand the Student Network Usage Agreement Form, and understand that this agreement will be in effect until rescinded by me, the undersigned. I DO NOT give my permission for my child to use Suwannee County Schools' technology network to access the internet.

**ELECTRONIC DISTRIBUTION OF STUDENT DATA**

☐ **YES** I DO give my permission for my child to have his/her name, picture, or other personal data included in photographs or videos that are in newspapers and newsletters or posted on school/district maintained or school/district sponsored websites or other electronic communication systems that will be subject to public viewing on the internet. I understand that this agreement will be in effect until rescinded by me, the undersigned. **OR**

☐ **NO** I DO NOT give my permission for my child to have his/her name, picture, or other personal data included in photographs or videos that are in newspapers and newsletters or posted on school/district maintained or school/district sponsored websites or other electronic communication systems that will be subject to public viewing on the internet. I understand that this agreement will be in effect until rescinded by me, the undersigned.

\_\_\_\_\_  
Parent/Legal Guardian Signature

\_\_\_\_\_  
Date

**STUDENTS GRADE 6<sup>TH</sup> – 12<sup>TH</sup> ONLY**

I understand and will abide by the provisions and conditions of the Student Network Usage Agreement Form. I understand that any violations of the above provisions may result in disciplinary action, the revocation of my access privileges, and/or appropriate legal action. I also agree to report any misuse of the network/information system to a school representative. All the rules described in the IT Policies and Procedures, the Student Code of Conduct, and the Suwannee County School Board Policies/Rules are applicable when I am on the network/internet.

\_\_\_\_\_  
Student Signature

\_\_\_\_\_  
Date

\_\_\_\_\_  
School Site

\_\_\_\_\_  
Grade





**Suwannee District Schools IT Department**

**Non-Student Guest Access and Usage Agreement Form**

The Suwannee County School District (SCSD) welcomes anyone whose intentions it is to better the lives and education of our students. In this effort we have created policies regarding the use of laptops and other electronic equipment not belonging to the SCSD on the SCSD network.

Using the SCSD network is a privilege. As with all privileges, it is the responsibility of the user to use this service appropriately and in compliance with all school board policies and procedures, Florida state law, and Federal laws.

The use of excessive bandwidth, reproduction of copyrighted materials, and attempts to circumvent or defeat mechanisms put in place by the SCSD staff to manage the network is strictly forbidden and will result in the termination of network services.

The SCSD assumes no responsibility for costs associated with loss or damage to devices not owned by SCSD on the SCSD network. The SCSD staff can provide support in aspects of network connectivity and access of SCSD network resources. Backing up data and ensuring the security of network devices is the sole responsibility of the owner.

The SCSD has the right to rescind privileges and or change this policy in the future.

Please sign below to acknowledge that you have read, understand, and agree to adhere to these policies.

Guest Name: \_\_\_\_\_

Date: \_\_\_\_\_

Signature: \_\_\_\_\_