



SARASOTA
COUNTY SCHOOLS

Information Technology Guidelines and Procedures

Sarasota, Florida

Revised August 2013

TABLE OF CONTENTS

- [Introduction](#)4
- [Access to Information Technology Resources](#)
 - Eligibility4
 - Account Activation/Termination4
 - Convention For User Account.....5
 - Management of Internet Bandwidth.....5
 - Reporting Critical Service Outages During Normal Working Hours.....5
 - Personal Technology on the Network6
 - Virus Protection6
 - Network Connections in Departments6
 - Dial-Up Connections6
 - Employee Departure Checkout Checklist.....7
- [Security](#)
 - Security on Data Networks8
 - User IDs and Passwords.....8
 - Protecting Desktop Equipment and Files8
 - Confidentiality and Privacy8
 - Central Computer Operations9
 - Responsible Use of Networks and Computing Facilities9
 - Individual Responsibility10
 - Logging In10
 - Institutional Privileges10
 - Legal Compliance10
- [Wireless Security Access Guidelines and Agreement](#)
 - Purpose11
 - Scope11
 - Supported Technology12
 - Appropriate Use.....12
 - Non-Compliance14
- [Network Security Guidelines for Portable Computers](#)
 - Introduction14
 - Protecting the Laptop14
 - Laptop User’s Responsibilities14
 - Security Audits.....14
- [Computer Hardware & Software](#)
 - Replacement of School Based Computer Equipment.....15
 - Replacement of Departmental Based Computer Equipment.....15
 - Inventory of Equipment.....16

Grant and School Funded Equipment	16
Printers and Other Peripheral Equipment	16
Responsibility for Equipment	16
Upgrades and Renewal	16
Repair of Computer Equipment	
Sarasota County Schools Computer Equipment	17
Personally Owned Equipment.....	17
Hardware Standards	17
Software Standards	
Rationale.....	17
Improved Data Sharing	17
Improved Support	18
Improved Training	18
Smoother Software Installations and Upgrades.....	18
Licensing of Software	18
Software on Personally Owned Equipment	19
Printer Guidelines	
Purpose	19
Scope	19
Supported Printers	19
General Guidelines	19
IT Asset Disposal Guidelines	
Purpose	21
Scope	21
Definitions.....	21
Guidelines	22
Practices	22
Information Technology Standards.....	23

Communications

Telephone and Voicemail

Purpose.....	24
Scope.....	24
Telephone and Voicemail Services.....	24
Basic Guidelines.....	24
Unacceptable Use.....	25
Limited Personal Acceptable Use	26
Monitoring.....	27
Service and Repair.....	27
Telephone Procedures.....	27
Voicemail Procedures.....	27

Electronic Mail (E-Mail)

Department or Group Accounts.....	27
Appropriate Use of E-mail.....	28

<u>Mobile Device Usage Guidelines and Agreement</u>	
Purpose.....	28
Scope.....	29
Guidelines and Appropriate Use.....	29
Non-Compliance.....	31

[End-User Backup Guidelines](#)

Introduction	31
Scope	32
Backup Schedule	32
Data Storage	32
Managing Restores.....	32

[Copyright on Digital Information Systems](#)

Introduction.....	33
Indemnification of Sarasota County Schools.....	34
Noncompliance and Sanctions.....	34
Malicious Misuse.....	34
Unacceptable Use of Software and Hardware.....	34
Inappropriate Access.....	35
Inappropriate Use of Electronic Mail and Internet Access.....	35

APPENDICES

A. <u>Anti-Virus Guidelines</u>	36
B. <u>Acceptable Use Policy</u>	39
C. <u>Password Guidelines</u>	42
D. <u>Technology Service Desk</u>	46

Introduction

This document establishes computer usage guidelines for Sarasota County Schools. Sarasota County Schools offers a wide array of computing, networking, and telecommunications resources and services to employees and students of the district. These services are in place to facilitate teaching and learning, research, and administrative activities to further the Sarasota County Schools mission. This document contains Information Technology guidelines and procedures while outlining responsibilities of those who use computing and networking facilities at the school district and beyond. Users of these services agree to abide by and be subject to the terms and conditions contained in this and all other applicable School District policies. Some departments on campus may have additional facilities, practices, and guidelines that apply to use of computing facilities in those departments. These guidelines are designed to enable high quality services and maximize productivity while protecting the rights of all members of the community.

Access to Information Technology Resources

Eligibility

Information Technology (IT) Resources (computer hardware, software, telephone systems, networks, services, data, and other information) are made available at the Sarasota County Schools to support and facilitate the teaching, research and administrative functions of the school district. Access to these resources is provided to administration, staff, and enrolled students consistent with their responsibilities. Under no circumstances may anyone use Sarasota County Schools IT resources in ways that are illegal (e.g. copyright violations), or interfere with reasonable use by other members of the Sarasota County Schools community. Other individuals, upon submission of a request, may be granted access to some, or all, of Sarasota County Schools IT resources by the Superintendent of Sarasota County Schools or designee. The terms of access will be stated at the time access is granted.

Account Activation/Termination

Access to Sarasota County Schools resources (such as email and network access) is controlled through individual accounts and passwords. Each user of the Sarasota County Schools electronic mail system is required to read and accept the Acceptable Use Policy each year. It is the responsibility of the employee to protect the confidentiality of their account and password information.

Convention For User Accounts

A network username will be generated for staff members during the hiring process through the Human Resources Department.

Management of Internet Bandwidth

The campus network, including our connection to the Internet, is a critical shared resource for supporting the academic programs. Uses of our internet connection that are central to the academic/administrative mission of the Sarasota County Schools (e.g. access to Sarasota County Schools web, e-mail, on-line testing, and other resources) will receive higher priority during times when classes are in session and offices are open (i.e. critical times). Low priority uses will receive lower priority during critical times. Between the hours of 7:00 a.m. and 4:00 p.m. each day (critical times) access to the Sarasota County Schools email and web servers from off campus is the highest priority. Incoming or outgoing web traffic between the Internet and the campus network is the next highest priority. The quality and volume of our Internet traffic is regularly monitored to assure that critical applications are available to members of the Sarasota County Schools community. Sarasota County Schools does monitor the content of traffic on the network. It is the responsibility of each person using Sarasota County Schools resources, including the network, to do so in an ethical and legal manner. Particular attention should be given to observing copyright laws for digital materials.

Reporting Critical Service Outages During Normal Working Hours

During normal business hours (Monday - Friday, 7:00 a.m. - 5:00 p.m.), employees of the Sarasota County Schools should notify the Technology Service Desk of suspected problems with computers, networks, and related Information Technology resources. IT will investigate the problem and determine corrective action. Resolution of critical service outages (defined below) will be a top IT Department priority and will be resolved in a timely manner. Non-critical problems will be investigated and resolved as quickly as possible. Outside of business hours and on district holidays suspected critical service outages should be reported with an email to the Technology Service Desk (See Appendix D). No employee of the district should call IT Department staff outside of normal business hours. Outside of these times, suspected critical service outages should be reported at the next designated time the following day. A critical service outage is defined as one or more of the following:

1. Failure of the district network equipment or internet connection making it impossible for a majority of users to access district resources.
2. Failure of the district web server affecting the entire district.
3. Failure of the district telephone system making it impossible for a majority of users to make outgoing calls or receive incoming calls.

4. Failure of the district e-mail system affecting the entire district.
5. Failure of the district HR, Finance and Student Information System.

Personal Technology on the Network

The rules and regulations contained in this pertaining to electronic mail and internet access are equally applicable to the use of personal devices. If bandwidth or other problems occur, IT reserves the right to discontinue access to the device. Computers connected to the network may not be used as servers for private enterprises, commercial activity, or personal profit. Computers connected to the network may not be used to provide access to the Internet for anyone not formally affiliated with the Sarasota County Schools. Personal computers are not to be used as servers. IT reserves the right to disconnect any network port whose activity causes an adverse effect on the network or on any other user. Network connections may also be revoked in the case of malicious or inappropriate computing activity on the network. IT reserves the right to restrict access to the network for diagnostic and maintenance services. Every effort will be made to provide advance notification and schedule such disruptions during times of minimum impact and traffic.

Virus Protection

All Sarasota County Schools computers will have virus protection installed. IT requires all personal computers and devices to install anti-virus software on their personal computers before the computer is given a network address. Failure to maintain such virus protection will result in the loss of connectivity to the Sarasota County Schools network until anti-virus software is installed. Anti-virus software on personal computers is required to be kept updated and is the sole responsibility of the user. (Appendix A)

Network Connections in Departments

All offices, laboratories, and classrooms on campus are wired for access to the network. If additional network jacks, or if network connections need to be moved to different locations, the school/department should request this service through the Technology Service Desk (Appendix D). Network connections, wiring, equipment, or jacks may not be altered or extended beyond the location of their intended use.

Dial-Up Connections

For all campus users the primary access to Sarasota County Schools computing services is through the campus network. Dial-in access via modem is not provided or permitted.

Employee Departure Checkout Checklist

This checklist explains the employee departure checkout process. Follow these steps for any employee departure, whether voluntary or involuntary. This checklist assumes that appropriate written notification of pending departure has either been supplied by the employee in the event of resignation, or will be supplied to the employee in the event of termination.

1. Notify the Technology Service Desk in advance that an employee will be departing so appropriate security measures can be taken. If the employee is being terminated, notify the Technology Service Desk that all of the employee's accounts (network, e-mail, voice) will need to be deactivated at a particular date and time. Ideally, deactivation should take place while the employee is being notified of his or her termination.
2. List in advance any equipment and files that should be in the employee's possession and must be returned.
3. Prior to an employee's last day, the following must be addressed:
 - Review any confidentiality and non-disclosure requirements. Remind employee that all files and documents are property of Sarasota County Schools and cannot be destroyed, removed, modified, or copied without approval from the direct supervisor.
 - Ensure return of all company property to the employee's supervisor, or make arrangements for its immediate return. Company property includes all keys, access cards, identification cards, credit cards, tools, books, reference materials, software, and equipment (such as laptop computers, tablets, pagers, and cell phones).
 - Gather and/or confirm the employee forwarding information, including home address and e-mail address (if appropriate).
 - Have the employee disclose all usernames and passwords to all accounts and/or applications to the employee supervisor for records management and redistribution purposes.
 - Review the status of any and all projects or work in progress.
 - Have the employee disclose the location of key work-related documents and records.
4. Have all work-related computer files transferred to cost center head for secure review. These files will be deleted, stored, or forwarded to the appropriate Sarasota County Schools staff member.
5. Arrange for return of personal print and computer files to the employee.
6. Arrange for the departing employees e-mail and phone calls to be temporarily forwarded to the employee's supervisor.

Security

Security on Data Networks

Security for access to the data network and to files or applications on a server is implemented via user ID and password systems. Each user is responsible for all e-mail transactions made under the authorization of his or her ID and password, and for all network e-mail activity originating from that connection. Users are personally responsible for the security of the ID and password assigned to them. Viewing, copying, altering or destroying any file, or connecting to a computer on the network without explicit permission of the owner is prohibited. Users may not use the Sarasota County Schools data network or telephone system to attempt to circumvent protection schemes or exercise security loopholes in any computer, network, or telephone system component.

User IDs and Passwords

Passwords should be known only to the person responsible for the account and user ID. Ways to ensure this include: avoiding storing passwords or any other information that could be used to gain access to other computing resources on your workstation; never sharing passwords, and never taping passwords to a wall, under a keyboard, or in other easily discoverable areas. Access to user IDs may not be loaned or sold and any suspected breach of password security should be immediately reported to the Technology Service Desk. See Password Guidelines in Appendix C.

Protecting Desktop Equipment and Files

Backups and protection of files stored on desktop equipment are the responsibility of the user of that equipment. Users must back up their work files on a regular basis. Department members are responsible for ensuring that critical files are backed up in their areas. Individual users are responsible for safeguarding the equipment entrusted to them by Sarasota County Schools. This includes reasonable protection of equipment from damage and theft. Individual users are also responsible for safeguarding any equipment they own personally and bring to campus.

Confidentiality and Privacy

Sarasota County Schools takes reasonable steps to protect users from unauthorized entry into their accounts or files, whether by other users or by system administrators, except in instances where a system-related problem requires such entry. A limited number of authorized Sarasota County School personnel must occasionally monitor information on the network and/or computer systems to maintain the integrity of the systems. This access is required for reasons that include, but are not limited to: trouble-shooting hardware and software problems; preventing unauthorized access and system misuse; providing for the overall efficiency and integrity of the systems;

protecting the rights and property of Sarasota County Schools; ensuring compliance with software and copyright, distribution, and other district guidelines concerning the use of the computer network; and complying with legal and regulatory requests for information.

System monitoring is a mechanism for keeping track of computer system activities, rather than a method for accessing private information. IT Department personnel also take reasonable steps to prevent the dissemination of information concerning individual user activities. It is the policy of the IT Department to disclose neither the contents of electronic mail and data files stored in or transmitted via the Sarasota County Schools Computer System nor the activities of individuals on the campus network to other individuals within or outside the Sarasota County Schools in the absence of a court order, or other legal mandate, or permission of the owner, or as governed under Florida's Sunshine Law. Private communication via computer is treated with the same degree of protection as private communication in other media. However, due to limitations of current technologies, which are inadequate to protect against unauthorized access, the confidentiality of e-mail and other system files cannot be assured. All users should be aware of this and use reasonable caution when transmitting confidential materials.

Central Computer Operations

Access to computer operations areas is restricted to those responsible for operation and maintenance. Computing facilities on campus are secured when not open for business. The IT Department takes action to provide reasonable protection against environmental threats such as flooding, lightning, extreme temperatures, and loss or fluctuation of electrical power for central server and network facilities. The IT Department maintains procedures for protecting critical data that reside on central servers. While the IT Department provides security for files stored on central computing facilities, it cannot be responsible for protection against floods, fires, and catastrophic events of this type. The IT Department does not guarantee the availability of backups for the restoration of files deleted through user error.

Responsible Use of Networks and Computing Facilities

Sarasota County Schools is a public institution fully committed to the ideals of academic freedom, freedom of expression, and cultural diversity. At the same time, inappropriate behavior and malicious misuse of computing resources that in any way degrades the district equipment and services or violates the rights of others in the district is strictly prohibited.

Individual Responsibility

While the IT Department is responsible for monitoring the use of computer systems, it is also the responsibility of all individuals in the Sarasota County Schools to urge their peers and colleagues to use the network and systems appropriately. This is the only way that the integrity and availability of the network and systems can be ensured for everyone. Each employee of the Sarasota County Schools is responsible for using only those accounts or computers for which he or she has authorization and is responsible for protecting all passwords. Individual responsibility includes respecting the rights of other users. Individuals are urged to report unauthorized use of computers, networks, or other IT Department facilities on campus by calling the Technology Service Desk.

Logging In

All students, employees, and individuals will see the below message each time they log into a computer.

This is a private computer system and is the property of Sarasota County Schools. It is for authorized use only. Users have not explicit or implicit expectation of privacy. Any or all users of this system maybe be intercepted, monitored, recorded, copied, audited, inspected and disclosed to management and law enforcement personnel if applicable. By using this system, the user consents to the aforementioned practices at the discretion of management. Unauthorized or improper use of this system may result in administrative disciplinary action and or civil and criminal penalties. By continuing to use this system you indicate you are aware and consent to these terms and conditions of use. DO NOT LOGON if you do not agree to the conditions stated above.

Institutional Privileges

Sarasota County Schools reserves the right to allocate resources in different ways in order to achieve maximum usage. To accomplish this, the system administrators may suspend or terminate privileges of individuals without notice if malicious misuse or use inconsistent with this documentation, any other district documentation, or applicable law is discovered. Privileges may also be suspended, without notice, to meet time dependent, critical operational needs. System administrators may also limit the number of messages or files that each user has in order to keep the system functioning.

Legal Compliance

All existing federal and state laws and district regulations and policies apply to the use of computing resources. All users of such resources are required to be in compliance with all laws, regulations and policies at all times. This

includes not only those laws and regulations that are specific to computers and networks, but also those that apply generally to personal conduct.

Wireless Security Access Guidelines and Agreement

Purpose

The purpose of this is to define standards, procedures, and restrictions for connecting to Sarasota County Schools internal network(s) or related technology resources via any means involving wireless technology. This can include, but is not limited to, access from the following:

- External hosts via remote access technology (for example, using a wireless router at home to connect to the Sarasota County Schools Virtual Private Network).
- Wireless gateways on Sarasota County Schools premises.
- Third-party wireless Internet service providers (also known as “hotspots”).

This applies to any equipment used to access Sarasota County Schools resources, even if said equipment is not Sarasota County Schools, owned, or supplied. For example, use of a public library's wireless network to access the Sarasota County Schools network would fall under the scope of these guidelines. The overriding goal of this is to protect Sarasota County Schools technology-based resources (such as Sarasota County Schools data, computer systems, networks, databases, etc.) from unauthorized use and/or malicious attack that could result in loss of information, damage to critical applications, loss of revenue, and damage to our public image. Therefore, all users employing wireless methods of accessing Sarasota County Schools technology resources must adhere to district-defined processes for doing so.

Scope

This applies to all Sarasota County Schools employees, including full-time staff, part-time staff, contractors, freelancers, and other agents who utilize district-owned, personally-owned, or publicly-accessible computers to access the organizations data and networks via wireless means. Wireless access to enterprise network resources is a privilege, not an entitlement. Consequently, employment at Sarasota County Schools does not automatically guarantee the granting of wireless access privileges. Wireless networks should not be considered a replacement for a wired network. They should be seen solely as extensions to the existing wired network, and are to be used for general purpose access in areas of transient use, such as common areas or meeting rooms. Wireless segments should not be used for work sessions involving any form of access to sensitive data. Addition of new wireless access points within Sarasota County Schools facilities will be managed at the sole discretion of IT. Non-sanctioned installations of wireless equipment or use of unauthorized equipment within the organizational

campus, is strictly forbidden. This is complementary to any previously-implemented guidelines dealing specifically with network access and remote access to the enterprise network.

Supported Technology

All wireless access points within the Sarasota County Schools firewall will be centrally managed by the IT Department and will utilize encryption, strong authentication, and other security methods at IT's discretion. Although IT is not able to manage public wireless resources, end-users are expected to adhere to the same security protocols while utilizing this equipment. Failure to do so will result in immediate suspension of all network access privileges so as to protect the district's infrastructure.

Appropriate Use

It is the responsibility of any employee of Sarasota County Schools who is connecting to the network via wireless means to ensure that all components of his/her wireless connection remain as secure as his or her network access within the office. It is imperative that any wireless connection used to conduct Sarasota County Schools business be utilized appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that users account. Based on this, the following rules must be observed:

1. General access to the organizational network through the internet by residential remote users through Sarasota County Schools network is permitted. However, the employee and student members using the internet for recreational purposes through company networks are not to violate any of Sarasota County Schools' internet acceptable use policies.
2. Employees using wireless access methods will, without exception, use secure remote access procedures. This will be enforced through public/private key encrypted strong passwords in accordance with Sarasota County Schools' password guidelines. Employees agree to never disclose their passwords to anyone, particularly to family members.
3. All remote computer equipment and devices used for business interests, whether personal- or district-owned, must display reasonable physical security measures. Users are expected to secure their Sarasota County Schools connected machines when they are physically at their machines, as well as when they step away. District owned computers will have installed district supplied antivirus software. Antivirus signature files must be updated in accordance with district guidelines. (Appendix A)
4. Due to the potential for bandwidth conflicts within the Sarasota County Schools campus, use of unsanctioned equipment operating within the 2.4 GHz range is strictly forbidden. If you have a need to use such

- equipment – for example, a cordless phone – please consult IT before proceeding further.
5. Prior to initial use for connecting to the Sarasota County Schools network, all public hotspots must be registered with IT.
 6. Remote users using public hotspots for wireless internet access must employ for their devices a district-approved and district provided VPN, and any other security measure deemed necessary by the IT Department. VPNs supplied by the wireless service provider will not be allowed.
 7. Hotspot and remote users must disconnect wireless cards when not in use in order to mitigate attacks by hackers, war drivers, and eavesdroppers.
 8. Users must apply new passwords every business/personal trip where district data is being utilized over a hotspot wireless service, or when a district device is used for personal Web browsing.
 9. Any remote connection (i.e. hotspot, ISDN, frame relay, etc.) that is configured to access Sarasota County Schools resources must adhere to the authentication requirements of Sarasota County Schools IT Department. In addition, all hardware security configurations (personal or company-owned) must be approved by Sarasota County Schools IT Department.
 10. Employees, contractors, and temporary staff will make no modifications of any kind to district-owned and installed wireless hardware or software without the express approval of the IT Department.
 11. Employees, contractors, and temporary staff with wireless access privileges must ensure that their computers are not connected to any other network while connected to Sarasota County Schools network via remote access.
 12. The wireless access user agrees to immediately report to his/her manager and the IT Department any incident or suspected incidents of unauthorized access and/or disclosure of company resources, databases, networks, and any other related components of the organizations technology infrastructure.
 13. The wireless access user also agrees to and accepts that his or her access and/or connection to Sarasota County Schools networks may be monitored to record dates, times, duration of access, data types and volumes, etc., in order to identify unusual usage patterns or other suspicious activity. As with in-house computers, this is done in order to identify accounts/computers that may have been compromised by external parties.
 14. IT reserves the right to turn off without notice any access port to the network that puts the districts systems, data, users, and clients at risk.

Non-Compliance

Failure to comply with the Wireless Security Access Guidelines and Agreement may result in the suspension of remote access privileges, disciplinary action, and possibly termination of employment.

Network Security Guidelines for Portable Computers

Introduction

Portable computers offer staff the ability to be more productive while on the move. They offer greater flexibility where and when staff can work and access information, including information on our Sarasota County Schools network. However, network-enabled portable computers also pose the risk of data theft and unauthorized access to our Sarasota County Schools network. Any device that can access the Sarasota County Schools network must be considered part of that network and therefore subject to guidelines intended to protect the network from harm.

Protecting the Laptop

In order to qualify for access to our Sarasota County Schools network, the laptop must meet the following conditions: Network settings, including settings for our VPN, must be reviewed and approved by IT support personnel. Anti-virus software must be installed. Software must have active scanning and be kept up-to-date.

Laptop User's Responsibilities

The user of the laptop is responsible for network security of the laptop whether they are onsite, at home, or on the road. The user of the laptop is responsible for keeping their anti-virus scanning software up-to-date at all times. It is strongly recommended that they update their anti-virus software before going on the road. The user of the laptop shall access network resources via a VPN connection. Use of public internet services is discouraged, as they do not offer adequate protection for the user.

Security Audits

The IT Department reserves the right to audit any laptop used for district business to ensure that it continues to conform to this certification. The IT Department will also deny network access to any laptop, which has not been properly configured and certified.

Computer Hardware & Software

Replacement of School Based Computer Equipment

All Sarasota County Schools school based computer equipment is on a regular replacement cycle of 5 years for computers and servers. Computer equipment is generally replaced during the summer months. During the spring, IT staff meets with schools to finalize needs and computers to be replaced. The goals of the replacement plan are to:

1. Assure that appropriate computing resources are available in schools to support the mission of the Sarasota County Schools.
2. Assure that each school faculty and staff member who uses computing resources in his or her position has a computer of sufficient capability to fulfill his/her responsibilities.
3. Implement minimum standards for computing equipment in schools, and encourage planning, cost-effective installation of new equipment and disposal of old equipment.

Sarasota County Schools school based computers are divided into three categories: Lab Computers - Will be replaced every five years, pending funding. Staff Computers - Will be replaced every five years, pending funding. Classroom Computers - Will be replaced every five years, pending funding.

Each computer in the replacement plan is designated as being in one of these three groups with a tentative date indicated for replacement. Administration, staff and teachers will have one Sarasota County Schools computer provided for them on the replacement plan. Computers will be provided to faculty replacements from a pool of computers designated for this purpose. Computers can be purchased from school budgets via a waiver approved by the Superintendent or designee. Computers purchased with grants or special one-time funding will not be on the replacement plan and must include a support plan along with the purchase. Any computer purchased with school budgets will be models pre-negotiated by the IT department.

Replacement of Departmental Based Computer Equipment

All departmental based computers will be replaced every five years pending funding. Computers can be purchased from departmental budgets via a waiver approved by the Superintendent or designee. Any computer purchased with department budgets will be models pre-negotiated by the IT department.

Inventory of Equipment

All Sarasota County Schools computers are maintained in a central inventory. At the time a computer enters the inventory the replacement cycle, if any, is designated. Old equipment is either donated to the Texcellence program or sold at auction by the Materials Management department.

Grant and School Funded Equipment

Individuals pursuing grants for computing equipment should discuss their plans with the Director of IT as part of the budgeting process. Computing equipment that is acquired under grants will enter the inventory and be upgraded on a regular replacement cycle only if approved at the time of the application for the grant. Some schools or departments may have funds available to them to purchase additional computer equipment. Such equipment should be ordered through the Sarasota County Schools purchasing process and will not normally be upgraded or replaced by the IT department. If this equipment is to be on the computer replacement plan the individual seeking the grant must obtain a commitment, in writing, from the Director of IT indicating this. Otherwise, the equipment will not be on a replacement cycle.

Printers and Other Peripheral Equipment

The Sarasota County Schools IT department provides networked printing locations and print servers in every school. Networked printers and/or copy machines are recommended. Individual desktop printers are not recommended. Other peripheral pieces of equipment such as scanners are also generally provided in clustered locations instead of individual offices. Since these pieces of equipment are usually used intermittently, clustering allows sharing of specialized technical resources. All purchases of printers and other peripherals devices are the responsibility of the said cost center.

Responsibility for Equipment

Each employee is responsible for taking reasonable safety precautions in regard to Sarasota County Schools owned computer equipment. Employees will be held responsible for damage to such equipment arising out of their negligence or intentional misconduct.

Upgrades and Renewal

For computer equipment on the replacement plan IT staff members consult with users prior to ordering and installing new equipment to determine the current and anticipated equipment needs. Machines that are replaced are returned to IT. IT then reassigns the machines, donates them to the Texcellence program or are sold at auction by the Materials Management department.

Repair of Computer Equipment

Sarasota County Schools Computer Equipment

All Sarasota County Schools computer equipment is maintained either in-house for out of warranty issues or through the manufacturer for in-warranty issues. If a hardware problem is suspected the user should submit a work request to the Technology Service Desk or call (861-4357) during normal business hours for assistance. If hardware service is indicated, arrangements will be made with the technician.

Personally Owned Equipment

Sarasota County Schools is not in any way responsible for personally owned equipment.

Hardware Standards

The following guidelines for standards are based on the current technology available combined with the current needs of the end-user today.

The primary considerations for each configuration (desktop, printing, portable computing) are:

1. Ease of connectivity to the Sarasota County Schools network.
2. Consistent performance of all integrated components in our network environment.
3. Industry leader with an established track record in manufacturing, sales and service
4. Successful in-house experience with the chosen product and configuration
5. Serviceability by the IT Department
6. The machine has a minimum lifetime of five years.

Software Standards

Rationale

In Sarasota County Schools modern networked environment, the ability to easily share information is important. Ideally, the ease of sharing should not depend upon which hardware environment is being used on the desktop. Central to making sharing facile is the software environment, particularly software used for word processing, spreadsheets, databases, network browsing, and electronic mail. The following are advantages of district-wide software standards:

Improved Data Sharing

Consistency of file formats provides for optimal file sharing capabilities between individuals, departments, and groups across the district. Identical resources on each desktop (schools and departments) provide ease of transferability and a consistent tool-set for all users, from any room

or office needed resources will be available. Sharing of data between applications (word processors, spreadsheets and data bases) is seamless. This would relieve an individual or cost center from the time consuming tasks of choosing a product, tracking down the best pricing and product availability, and generating the proper paperwork to place an order for the product. Significant savings can be achieved through site licenses or quantity discounts.

Improved Support

IT support personnel can focus on depth of application knowledge rather than breadth of numerous applications. Product expertise means questions can be answered more quickly and efficiently. Support efforts can be focused on supporting the end-user and documenting known problems. Support could come from any member of the Sarasota County Schools community, since most will be using the same application.

Improved Training

Training teams can focus on developing curricula for levels of user proficiency (introductory, intermediate and advanced). Training specialists from outside the district can be used more effectively and economically.

Smoother Software Installation and Upgrades

Software installations for new machines are invisible to the users by making it part of the hardware installation. Installations are now routine, rather than a specialized process for each individual, resulting in time savings. Installations and upgrades are made available to all users via the campus network, and automated for consistency. Upgrades can be tested and documented prior to campus-wide deployment to reduce potential incompatibility and problems. Simplified software licensing is achieved through district wide license purchases.

Licensing of Software

The use of all software in the district is protected by copyright laws and must be used in accordance with software licenses. It is against district guidelines to copy or reproduce any licensed software. Unlicensed software may not be installed on any computers owned by the Sarasota County Schools . The unauthorized use or copying of software is a serious violation and subject to disciplinary action. Such unauthorized use or copying may also subject the offending individual to lawsuits by third parties.

Software on Personally Owned Equipment

Sarasota County Schools educational licensing agreements for software specifically limit installation to machines owned by the district. Therefore, software purchased by the Sarasota County Schools under these agreements may not be installed on personally owned equipment. For information on these programs, Sarasota County Schools current licensing agreements, and exceptions, contact the Director of the IT Department.

Printer Guidelines

Purpose

Printers represent one of the highest equipment expenditures at Sarasota County Schools. The goal of this is to facilitate the appropriate and responsible business use of Sarasota County Schools printer assets, as well as control Sarasota County Schools printer cost of ownership by preventing the waste of paper, toner, ink, and so on.

Scope

These Printer Guidelines apply to all employees and students of Sarasota County Schools, as well as any contract employees in the service of Sarasota County Schools who may be using Sarasota County Schools networks and equipment.

Supported Printers

Sarasota County Schools supports all network printers on the district network system. An effort has been made to standardize on specific printer models in order to optimize contractual agreements and minimize support costs.

General Guidelines

1. Printers are to be used for documents that are relevant to the day-to-day conduct of business at Sarasota County Schools. Sarasota County Schools printers should not be used to print personal documents.
2. Installation of personal printers is not recommended at Sarasota County Schools due to the cost of maintaining and supporting.
3. Do not print multiple copies of the same document – the printer is not a copier and typically costs more per page to use. If you need multiple copies, print one good copy on the printer and use the photocopier to make additional copies.
4. If you print something, please pick it up in a timely fashion. If you no longer want it, please dispose of it appropriately (i.e. recycle).

5. If you come across an unclaimed print job, please stack it neatly and turn into the main office. All unclaimed output jobs will be discarded after two days.
6. Make efforts to limit paper usage by taking advantage of duplex printing (i.e. double-sided printing) features offered by some printers and other optimization features (e.g. printing six PowerPoint slides per page versus only one per page).
7. Make efforts to limit toner use by selecting light toner and lower dpi default print settings.
8. Avoid printing large files, as this puts a drain on network resources and interferes with the ability of others to use the printer. Jobs in excess of 100 pages should be sent to the district Printing Shop.
9. If printing a job in excess of 25 pages, please be at the printer to collect it when it comes out to ensure adequate paper supply for the job and that the output tray is not overfull (i.e. you may need to remove some of the output before the print job is finished).
10. Avoid printing e-mail messages. This is wasteful. Instead, use the folders and archiving functionality in your e-mail application to organize and view your messages.
11. Avoid printing a document just to see what it looks like. This is wasteful.
12. Avoid re-using paper in laser printers, as this can lead to paper jams and other problems with the machine.
13. Many printers do not support certain paper types, including vellum, transparencies, adhesive labels, tracing paper, card stock, or thicker paper. If you need to use any of these paper types, consult with IT to find out which machines can handle these specialty print jobs.
14. Color printing is typically not required by general business users. Given this selective need, as well as the high cost per page to print color copies, the number of color-capable printers available has been minimized. You are strongly encouraged to avoid printing in color when monochrome (black) can be used.
15. Printer paper is available at all departments. Toner cartridges are available at all departments.

16. If you encounter a physical problem with the printer (paper jam, out of toner, etc.) and are not “trained” in how to fix the problem, please do not try. Instead, report the problem to the Technology Service Desk.

17. Report any malfunction of any printing device to the Technology Service Desk as soon as possible.

IT Asset Disposal Guidelines

Purpose

The purpose of this is to establish and define standards, procedures, and restrictions for the disposal of non-leased IT equipment in a legal, cost-effective manner. Sarasota County Schools surplus or obsolete IT assets and resources (i.e. desktop computers, servers, laptops, etc.) must be discarded according to legal requirements, environmental regulations and in accordance with the Materials Management Department guidelines. Therefore, all disposal procedures for retired IT assets must adhere to district-approved methods.

Scope

This applies to the proper disposal of all non-leased Sarasota County Schools IT hardware, including PCs, printers, handheld devices, servers, hubs, switches, bridges, routers, and so on. District-owned surplus hardware, obsolete machines, and any equipment beyond reasonable repair or reuse are covered by these guidelines. Where applicable, it is desirable to achieve some residual value of the IT asset in question through reselling, auctioning, donation, or reassignment to a less-critical function.

Definitions

“Non-leased” refers to any and all IT assets that are the sole property of Sarasota County Schools; that is, equipment that is not rented, leased, or borrowed from a third-party supplier or partner company. “Disposal” refers to the reselling, reassignment, recycling, donating, or throwing out of IT equipment through responsible, ethical, and environmentally sound means. “Obsolete” refers to any and all equipment over 5 years old and/or that which no longer meets requisite functionality. “Surplus” refers to hardware that has been replaced by upgraded equipment or is superfluous to existing requirements. “Beyond reasonable repair” refers to any and all equipment whose condition requires fixing or refurbishing that is likely to cost equal to or more than total replacement or 50% of current value.

Guidelines

Disposal and disposal procedures of all IT assets and equipment will be centrally managed and coordinated by Sarasota County Schools IT Department. The IT Department is also responsible for managing the removal of district data from all IT assets slated for disposal. The IT Department is in charge of selecting and approving external agents for recycling hardware and/or sanitizing hardware of harmful toxins.

Practices

Acceptable methods for the disposal of IT assets are as follows:

1. Donated to the Texcellence program.
2. Recycled and/or refurbished to leverage further use (within limits of reasonable repair).
3. Used as trade-in against cost of replacement item.

It is the responsibility of any employee of Sarasota County Schools IT Department with the appropriate authority to ensure that IT assets, equipment, and hardware are disposed of according to one or more of the methods prescribed above. It is imperative that any disposals performed by Sarasota County Schools are done appropriately, responsibly, and ethically, as well as with district resource planning in mind. The following rules must therefore be observed:

Obsolete IT Assets: As prescribed above, “obsolete” refers to any and all computer or computer-related equipment over 5 years old and/or equipment that no longer meets requisite functionality. Identifying and classifying IT assets as obsolete is the sole province of Sarasota County Schools IT Department under the guidelines of the Materials Management Department. Decisions on this matter will be made according to Sarasota County Schools purchasing/procurement strategies. Equipment lifecycles are to be determined by IT asset management best practices (i.e. total cost of ownership, required upgrades, etc.).

Reassignment of Retired Assets: Reassignment of computer hardware to a less-critical role is made at the sole discretion of Sarasota County Schools IT Department. It is, however, the goal of Sarasota County Schools to, whenever possible, reassign IT assets in order to achieve full return on investment (ROI) from the equipment and to minimize hardware expenditures when feasible reassignment to another business function will meet requisite functionality.

Trade-Ins: Where applicable, cases in which a piece of equipment is due for replacement by a newer model, reasonable actions must be taken to ensure that a fair and market trade-in value is obtained for the old IT asset against the cost of the replacement. Sarasota County Schools Purchasing

and Procurement manager or IT Asset manager will assume this responsibility.

Income Derived from Disposal: Whenever possible, it is desirable to achieve some residual value from retired or surplus IT assets. Any and all receipts from the sale of IT assets must be kept and submitted to the Finance Department. Income derived from the sale must be fully receipted and monies sent to Sarasota County Schools Finance Department.

Cannibalization and Assets Beyond Reasonable Repair: The IT Department is responsible for verifying and classifying any IT assets beyond reasonable repair. Equipment identified as such should be cannibalized for any spare and/or working parts that can still be put to sufficient use within the organization. The IT Department will inventory and stockpile these parts. Remaining parts and/or whole machines unfit for use will be disposed by appropriate means.

Decommissioning of Assets: All hardware slated for disposal by any means must be fully wiped clean of all data. Sarasota County Schools IT Department will assume responsibility for decommissioning this equipment by deleting all files, company-licensed programs, and applications using a pre-approved disk-sanitizer. This level 3 sanitizer must completely overwrite each and every disk sector of the machine with zero-filled blocks.

Harmful Substances: Hazardous materials such as lead, mercury, bromine, cadmium, etc. must be thoroughly removed from computer hardware before shipment to a landfill as rubbish. The IT Department may perform this action itself using government-approved disposal methods, or hire an accredited disposal company specializing in this service. No matter what the route taken, the removal and discarding of toxins from Sarasota County Schools equipment must be in full compliance with local and federal laws.

Donations: IT assets with a net residual value that are not assigned for reuse, discarding, or sale to external buyers, must be donated to the Texcellence program. All donations must be authorized by Sarasota County Schools.

Information Technology Standards

The Information Technology Standards lists all technologies supported by the organization and serves as a guideline for all technology purchasing and use decisions, including hardware, software, peripherals, and network

components. The primary goals of developing and implementing such standards are:

- To ease purchasing decisions by pre-evaluating and pre-approving technology solutions.
- To reduce training and support costs and create economies of scale by narrowing the number of technologies and products used.
- To ensure integration and interoperability between technologies.
- To set parameters for future technology innovation and development.

The following standard technologies were selected based on: prevalence in the organization; cases where two or more competing technologies previously existed; or on an assessment of relative quality and performance as dictated by business needs. Please refer to this document, which is located on the Purchasing Department's SharePoint site, when making a purchasing decision or when selecting technologies as part of a development project. Sections of this document may be extracted and used as part of project charters or other agreements where technology parameters should and must be set, such as in the case of contracted work.

Communications

Telephone and Voicemail

Purpose

Telephone communication is an essential part of the day-to-day operations of Sarasota County Schools. Telephone and voicemail services are provided to employees of Sarasota County Schools in order to facilitate performance of Sarasota County Schools work. The goal of this is to balance the business need for telephone and voicemail use by Sarasota County Schools with the costs involved.

Scope

This applies to all employees of Sarasota County Schools, and all usage of Sarasota County Schools telephone and voicemail services.

Telephone and Voicemail Services

Sarasota County Schools Telephone system consists of either a PBX system or Voice Over Internet Protocol system. The telephone system is part of the data network.

Basic Guidelines

As with all Sarasota County Schools resources, the use of telephones and voicemail should be as cost effectively as possible and in keeping with the

best interests of Sarasota County Schools. All employees must operate within the following basic guidelines. Further information on appropriate and inappropriate use follows this section.

- All telephones, telephony equipment, voicemail boxes, and messages contained within voicemail boxes are the property of Sarasota County Schools.
- The IT Department or a contracted vendor is responsible for installation and repair of all Sarasota County Schools telephony equipment and administration of telephone and voicemail accounts.
- Cost center heads are responsible for overseeing telephone and voicemail use and ensuring compliance, as well as ensuring IT is notified of any adds, moves, or changes required to telephone or voicemail services.
- All Sarasota County Schools employees are eligible to receive a telephone based on their needs.
- Employees that require direct lines are the key administrators. Examples would be the Superintendent, Executive Directors and Principals. This will be based on job function and approval by the Superintendent. All other employees will receive extensions based on their job function.
- Sarasota County Schools will limit the number of extensions and voicemail boxes because of the current configuration of the PBX system.
- The number of telephone calls made should be limited in number and duration to that necessary for the effective conduct of business. Efforts should be made to limit the length of telephone calls.
- All voicemail boxes will be protected with a PIN (personal identification number). PINs must be changed at least once a year to aid in mailbox security. PINs must not be shared with others.
- A voicemail box can hold 5 minutes of message storage time. If a voicemail box is full, no further messages can be recorded. Read voicemail messages will be up to the employee to delete after 7 days.
- Voicemail is to be used as a backup in the event you are not available to answer a call, and should not be used to “screen” calls. Each user is expected to respond to voicemail messages in a timely manner.
- If you will be away from the office for more than one business day, you are expected to change your voicemail greeting to reflect this fact and direct callers to alternate contacts if applicable.
- Use of directory assistance (i.e. 411) should be avoided since a fee is incurred with each use. If you are unsure of a number, please consult print or online telephone directories first.

Unacceptable Use

Sarasota County Schools telephone and voicemail services may not be used for the following:

- Transmitting obscene, profane, or offensive messages.
- Transmitting messages or jokes that violate our harassment policy or create an intimidating or hostile work environment.
- Breaking into a voicemail box via unauthorized use of a PIN or other password.
- Broadcasting unsolicited personal views on social, political, or other non-business related matters.
- Soliciting to buy or sell goods or services unrelated to Sarasota County Schools.
- Calling 1-900 phone numbers.
- Making personal long-distance phone calls without supervisor permission.

Misuse of telephone and voicemail services can result in disciplinary action, up to and including termination.

Limited Personal Acceptable Use

In general, personal use of telephone and voicemail services is allowable, but must be limited in number and duration and must not interfere with performance of official business duties. Limited personal acceptable use is allowed under the following circumstances:

- An employees work schedule changes without advance notice and the employee must notify a family member or make alternate transportation or childcare arrangements.
- Brief local calls to a spouse, minor child, or elderly parent, or to those responsible for them (e.g. school, daycare center, nursing home).
- The employee needs to make a call that can only be made during regular working hours, such as to a doctor or local government agency.
- The employee needs to make arrangements for emergency repairs to his or her residence or automobile.
- A call that reasonably could not be made at another time and is of moderate duration.

Any personal long-distance calls that must be made (excepting toll-free 1-800 calls) should be charged to the employees home telephone number, personal credit card, personal calling card, or be charged to the called party. If a personal long-distance call must be made that will be billed to Sarasota County Schools, the employee should first receive permission from their cost center head to make the call. Regardless, employees are expected to reimburse Sarasota County Schools for the cost of any long-distance calls within 2 days of receipt of the relevant bill.

Monitoring

Sarasota County Schools reserves the right to monitor telephone and voicemail use, including telephone conversations and the contents of voicemail boxes. Monitoring of telephone and voicemail use will only be done for legitimate reasons, such as to assess customer service quality assurance, retrieve lost messages, recover from system failure, or comply with investigations of wrongful acts. The following telephone and voicemail usage reports may be generated by Sarasota County Schools:

- Date, time, length of call, number called;
- Costs per call;
- Type of usage.

Service and Repair

The IT Department requires a five day notice to set up a standard telephone service and voicemail box. If there is a problem with an existing telephone or voicemail box, contact the Technology Service Desk. Fixes are typically made within 3 days.

Telephone Procedures

All employees that receive a telephone also receive the manual on how to operate their phone. It is the employee's responsibility to learn how to operate their phone. If an employee has lost their manual, they can contact the Technology Service Desk to receive another copy.

Voicemail Procedures

All employees are to follow Sarasota County Schools voicemail procedures. Voicemail setup procedures are in the manual you received with your telephone. If you have trouble in setting up your voicemail, you can contact the Technology Service Desk for help.

Electronic Mail (E-Mail)

Department or Group Accounts

By special permission, Sarasota County Schools employees will be granted a single account to facilitate connections between the department or group and interested parties. The department or group must identify one person to be responsible for the account and to act as the contact person. All employees of Sarasota County Schools are entitled to an e-mail account. E-mail accounts will be granted to third party non-employees on a case-by-case basis. Applications for these temporary accounts must be submitted in writing to the Sarasota County Schools Superintendent. All terms, conditions, and restrictions governing e-mail use must be in a written and signed agreement. E-mail access will be terminated when the employee or third party terminates their association with the Sarasota County Schools unless

other arrangements are made. Sarasota County Schools is under no obligation to store or forward the contents of an individual's e-mail inbox/outbox after the term of their employment has ceased.

Appropriate Use of E-mail

Sarasota County Schools strongly recommends that e-mail not be used for confidential communication. E-mail is now considered a formal written record that carries the same legal weight as a formal memorandum. Users of e-mail should remember that e-mail messages become the possession of the receiver and can be easily duplicated and redistributed by recipients. Messages that have been deleted can unintentionally be retained on system backup files and archives. In addition, even secure passwords are not completely confidential. When a private message needs to be conveyed between two individuals, a conversation is the best way to accomplish it, and messages that should not be preserved should be deleted immediately. Sarasota County Schools guidelines prohibit certain types of e-mail. These include mail that may be perceived as harassment, political campaigning, or commercial solicitation. Chain mail is also prohibited. Violators will be subject to loss of computer access privileges, as well as additional disciplinary action as determined by the Sarasota County Schools disciplinary procedures. Certain types of e-mail, including but not limited to harassing e-mail, may also subject the sender to civil or criminal penalties. In spite of Sarasota County Schools guidelines, e-mail can be abused by malicious users who know the owner's computing ID and password. Users are responsible for protecting their own passwords.

Mobile Device Usage Guidelines and Agreement

Purpose

The purpose of this is to define standards, procedures, and restrictions for connecting to Sarasota County Schools internal network(s) or related technology resources via any means involving mobile devices. This applies to, but is not limited to, all devices that fit the following device classifications:

- Mobile devices that are standalone (i.e. connectible using wired sync cables and/or cradles.)
- Devices that have integrated wireless capability. This capability may include, but is not limited to, Wi-Fi, Bluetooth, and IR.
- Smartphones.
- Any related components of Sarasota County Schools technology infrastructure used to provide connectivity to the above.
- Any third-party hardware, software, processes, or services used to provide connectivity to the above.

The guidelines apply to any mobile device hardware and related software that could be used to access Sarasota County Schools resources, even if said equipment is not Sarasota County Schools sanctioned, owned, or supplied. The overriding goal of this is to protect Sarasota County Schools technology-based resources (such as Sarasota County Schools data, computer systems, networks, databases, etc.) from unauthorized use and/or malicious attack that could result in loss of information, damage to critical applications, loss of revenue, and damage to our public image. Therefore, all users employing mobile device-based technology to access Sarasota County Schools technology resources must adhere to district-defined processes for doing so.

Scope

This applies to all Sarasota County Schools employees, including full- and part-time staff, contractors and other agents who utilize district-owned, personally owned, or publicly-accessible mobile device-based technology to access the organizations data and networks via wired and wireless means. Such access to enterprise network resources is a privilege, not a right. Consequently, employment at Sarasota County Schools does not automatically guarantee the granting of these privileges. Addition of new hardware, software, and/or related components to provide additional mobile device-related connectivity within Sarasota County Schools facilities will be managed at the sole discretion of IT. Non-sanctioned installations of mobile device-related hardware, software, and/or related components, or use of same within the organizational campus, or to gain access to organizational computing resources, are strictly forbidden. This is complementary to any previously implemented guidelines dealing specifically with network access, wireless access, and remote access to the enterprise network.

Guidelines and Appropriate Use

It is the responsibility of any employee of Sarasota County Schools who is connecting to the organizational network via a mobile device to ensure that all components of his/her connection remain as secure as his/her network access within the office. It is imperative that any wired (via sync cord, for example) or wireless connection, including, but not limited to mobile devices and service, used to conduct Sarasota County Schools business be utilized appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that users account. Based on this, the following rules must be observed:

- Employees using mobile devices and related software to connect to Sarasota County Schools technology infrastructure will, without exception, use secure remote access procedures. This will be enforced through public/private key encrypted strong passwords in accordance with Sarasota County Schools password guidelines. Employees agree

to never disclose their passwords to anyone, particularly to family members if business work is conducted from home.

- All mobile devices that are used for business interests, whether personal- or company-owned, must display reasonable physical security measures. Users are expected to secure all handhelds and related devices used for this activity whether or not they are actually in use and/or being carried. This includes, but is not limited to, power-on passwords.
- Any non-Sarasota County Schools computers used to synchronize with mobile devices will have installed whatever antivirus software deemed necessary by Sarasota County Schools IT Department. Antivirus signature files must be updated in accordance with existing District policy.
- Passwords and other confidential data as defined by Sarasota County Schools IT Department are not to be stored on mobile devices or their associated storage devices (such as SD and CF cards, as well as Memory Sticks and related flash-based supplemental storage media.)
- Due to the potential for bandwidth conflicts within the Sarasota County Schools campus, use of unsanctioned equipment operating within the 2.4 GHz range is strictly forbidden. If you have a need to use such equipment – for example, a wireless mobile device or smartphone – please consult IT before proceeding further.
- Remote users using non-Sarasota County Schools network infrastructure to gain access to Sarasota County Schools resources via their mobile devices must employ for their devices and related infrastructure a company-approved personal firewall, VPN, and any other security measure deemed necessary by the IT Department. VPNs supplied by the wireless service provider should also be used, but only in conjunction with Sarasota County Schools additional security measures. IT will support its sanctioned hardware and software, but is not accountable for conflicts or problems whose root cause is attributable to a third-party product.
- For wireless-enabled mobile devices, users must deactivate their devices when not in use in order to mitigate attacks by hackers, war drivers, and eavesdroppers.
- Users must apply new passwords every business/personal trip where company data is being utilized on or synchronized to a mobile device.
- Any mobile device that is configured to access Sarasota County Schools resources via wireless or wired connectivity must adhere to the authentication requirements of Sarasota County Schools IT Department. In addition, all hardware security configurations (personal or company-owned) must be approved by Sarasota County Schools IT Department.

- Employees, contractors, and temporary staff will make no modifications of any kind to district-owned and installed hardware or software without the express approval of Sarasota County School's IT Department. This includes, but is not limited to, installation of mobile device software on district-owned desktop or laptop computers, connection of sync cables and cradles to district-owned equipment, and use of district-owned wireless network bandwidth via these devices.
- Employees, contractors, and temporary staff with Sarasota County Schools sanctioned wireless-enabled mobile devices must ensure that their computers and handheld devices are not connected to any other network while connected to Sarasota County Schools network via remote access.
- The mobile device-based user agrees to immediately report to his/her manager and Sarasota County Schools IT Department any incident or suspected incidents of unauthorized access and/or disclosure of district resources, databases, networks, etc.
- The mobile device-based wireless access user also agrees to and accepts that his or her access and/or connection to Sarasota County Schools networks may be monitored to record dates, times, duration of access, etc., in order to identify unusual usage patterns or other suspicious activity. As with in-house computers, this is done in order to identify accounts/computers that may have been compromised by external parties.
- Sarasota County Schools will not reimburse employees for business-related wireless mobile device-based access connections made on a pre-approved privately owned ISP service.

Policy Non-Compliance

Failure to comply with the Mobile Device Usage Guidelines and Agreement may, at the full discretion of the Sarasota County Schools, result in the suspension of any or all-remote access privileges, disciplinary action, and possibly termination of employment.

End-User Backup Guidelines

Introduction

Data is one of Sarasota County Schools most important assets. In order to protect this asset from loss or destruction, it is imperative that it be safely and securely captured, copied, and stored. The goal of this document is to outline guidelines that governs how and when data residing on district desktop computers will be backed up and stored for the purpose of

providing restoration capability. In addition, it will address methods for requesting that backed up data be restored to individual systems.

Scope

This refers to the backing up of data that resides on computers and other such devices.

Responsibility for backing up data on local desktop systems or laptops rests solely with the individual user. It is imperative that end-users save their data to the appropriate media and/or network space outlined in these guidelines in order that their data is backed up regularly in accordance with district regulations. This does not cover end-user information that is saved on a network or shared drive, as these are backed up when the servers are backed up.

Backup Schedule

Incremental backups are conducted on a nightly basis with full backups completed weekly.

Data Storage

It is Sarasota County Schools procedure that ALL Sarasota County Schools data will be backed up according to schedule. This includes any district documentation (i.e. reports, RFPs, contracts, etc.), e-mails, applications/projects under development, and so on.

Sarasota County Schools data, especially works-in-progress, should be saved to the available network drive. This ensures that data will be backed up when the servers are backed up. If data is saved on a workstations local drive, then that must be backed up every week onto storage media such as CD Read/Write disks or some type removable storage device, such as a mini hard drive, data cartridge, or solid state memory card. Responsibility for backing up data on local desktop systems or laptops rests solely with the individual user.

Managing Restores

The ultimate goal of any backup process is to ensure that a restorable copy of data exists. If the data cannot be restored, then the process is useless. As a result, it is essential that the IT Department regularly test its ability to restore data from the storage media or network drive. As such, all storage media must be tested at least once every month to ensure that the data they contain can be completely restored to end-user workstations. Data will be restored from a backup if:

- There is an intrusion or attack.
- Files have been corrupted, deleted, or modified.

- Information must be accessed that is located on an archived backup.
- That workstation belongs to a domain.

In the event that an end-user requires or requests or needs a data restore, the following guidelines will be adhered to:

1. The individual responsible for overseeing backup and restore procedures is Manager of Telecommunications and Network Services. If a user has a restore request, they can contact the Technology Service Desk via a web browser, by calling or by sending an e-mail.
2. In the event of unplanned downtime, attack, or disaster, Sarasota County Schools full restoration procedures will be implemented.
3. In the event of a local data loss due to human error, the end-user affected must contact the Technology Service Desk and request a data restore. The end-user must provide the following information:
 - Name.
 - Contact information.
 - Name of file(s) and/or folder(s) affected.
 - Last known location of files(s) and/or folder(s) affected.
 - Extent and nature of data loss.
 - Events leading to data loss, including last modified date and time (if known).
 - Urgency of restore.
4. Depending on the extent of data loss, backup tapes and storage media may both need to be used. The timing in the cycle will dictate whether or not these tapes and/or other media are onsite or offsite. Tapes and other media must be retrieved by the server administrator or pre-determined replacement. If tapes and/or other media are offsite and the restore is not urgent, then the end-user affected may be required to wait for a cost-effective opportunity for the tape(s) and/or other media to be retrieved.
5. If the data loss was due to user error or a lack of adherence to procedure, then the end-user responsible may be required to participate in a tutorial on effective data backup practices.

Copyright on Digital Information Systems

Introduction

Individuals using computers and networks ("Digital Information Systems") at Sarasota County Schools are responsible for complying with copyright laws

and the districts guidelines and procedures regarding use of the Digital Information Systems.

Indemnification of Sarasota County Schools

Users agree, in consideration of access to the districts computing, networking and media services, to indemnify, defend, and hold harmless the Sarasota County Schools for any lawsuits, claims, losses, expenses or damages, including, but not limited to, the user's access to or use of the districts computing, networking, and media services and facilities.

Noncompliance and Sanctions

Information Technology Services may suspend or terminate all computing privileges of any individuals without notice who engage in improper computing activities. Serious cases, as determined by the Superintendent of the Sarasota County Schools, will be referred to the Sarasota County Schools for disciplinary action. Such disciplinary action may include the suspension or termination of the offending individual, as appropriate and as determined at the sole discretion of Sarasota County Schools. Where violation of state and federal law is involved, cases will be referred to the proper legal authorities for action. The following serves to provide examples of violations of computing or computing facility guidelines at Sarasota County Schools. The list of violations includes, but is not limited to:

Malicious Misuse.

Examples: Using IDs or passwords assigned to others, disrupting the network, destroying information, removing software from general use computers, spreading viruses, sending e-mail that threatens or harasses other people, invading the privacy of others, and subscribing others to mailing lists or providing the e-mail addresses of others to bulk mailers without their approval.

Unacceptable Use of Software and Hardware

Examples: knowingly or carelessly running or installing unlicensed software on any computer system or network; giving another user a program intended to damage the system; running or installing any program that places an excessive load on a computer system or network, or compromises the security of the systems or network; violating terms of applicable software licensing agreements, including copying or reproducing any licensed software; or violating copyright laws and their fair use provisions through inappropriate reproduction or dissemination of copyrighted text, images, or other materials; using imaging equipment to duplicate, alter and subsequently reproduce official documents.

Inappropriate Access

Examples: unauthorized use of a computer account; providing misleading information in order to obtain access to computing facilities; using the campus network to gain unauthorized access to any computer system; connecting unauthorized equipment to the campus network; unauthorized attempts to circumvent data protection schemes to uncover security loopholes (including creating and/or running programs that are designed to identify security loopholes and/or decrypt intentionally secure data); knowingly or carelessly performing an act that will interfere with the normal operation of computers, terminals, peripherals, or networks; deliberately wasting or overloading computing resources, such as printing too many copies of a document; or other activities.

Inappropriate Use of Electronic Mail and Internet Access

E-mail communications are subject to statements of conduct as well as all applicable federal and state laws. In addition, other activities that threaten the integrity of the system or harm individual users are not allowed. These include, but are not limited to initiating or propagating electronic chain letters; inappropriate mass mailing including multiple mailings to news groups, mailing lists, or individuals, forging the identity of a user or machine in an electronic communication or sending anonymous e-mail; using another person's e-mail account or identity to send e-mail messages; attempting to monitor or tamper with another user's electronic communications; reading, copying, changing, or deleting another user's files or software without the explicit agreement of the owner; or using e-mail to solicit or proselytize others for commercial ventures, religious or political causes, or for personal gain.

APPENDIX A



Anti-Virus Guidelines

Purpose

A virus is a piece of potentially malicious programming code that will cause some unexpected or undesirable event. Viruses can be transmitted via e-mail or instant messaging attachments, downloadable Internet files, flash drives and CDs. Viruses are usually disguised as something else, and so their presence is not always obvious to the computer user. A virus infection can be very costly to Sarasota County School Board in terms of lost data, lost staff productivity, and/or lost reputation. As a result, one of the goals of Sarasota County School Board is to provide a computing network that is virus-free. The purpose of this is to provide instructions on measures that must be taken by Sarasota County School Board employees to help achieve effective virus detection and prevention.

Scope

This applies to all computers that are connected to the Sarasota County School Board network via a standard network connection, wireless connection, modem connection, or virtual private network connection. This includes both district-owned computers and personally owned computers attached to the Sarasota County School Board network. The definition of computers includes desktop workstations, laptop computers, handheld computing devices, tablet computing devices, and servers.

General Guidelines

Currently, Sarasota County School Board has anti-virus software in use. Licensed copies of anti-virus software can be obtained from the IT Department. The most current available version of the anti-virus software package will be taken as the default standard. All computers attached to the Sarasota County School Board network must have standard, supported anti-virus software installed. This software must be active, be scheduled to perform virus checks at regular intervals, and have its virus definition files kept up to date. Any activities with the intention to create and/or distribute malicious programs onto the Sarasota County School Board network (e.g. viruses, worms, Trojan horses, e-mail bombs, etc.) are strictly prohibited. If an employee receives what he/she believes to be a virus, or suspects that a computer is infected with a virus, it must be reported to the Technology Service Desk immediately. Report the following information (if

known): virus name, extent of infection, source of virus, and potential recipients of infected material. No employee should attempt to destroy or remove a virus, or any evidence of that virus, without direction from the IT Department. Any virus-infected computer will be removed from the network until it is verified as virus-free.

Rules for Virus Prevention

1. Always run the standard anti-virus software provided by Sarasota County Schools.
2. Never open any files or macros attached to an e-mail from an unknown, suspicious, or untrustworthy source.
3. Never open any files or macros attached to an e-mail from a known source (even a coworker) if you were not expecting a specific attachment from that source.
4. Be suspicious of e-mail messages containing links to unknown Web sites. It is possible that the link is a malicious executable (.exe) file disguised as a link. Do not click on a link sent to you if you were not expecting a specific link.
5. Never copy, download, or install files from unknown, suspicious, or untrustworthy sources or removable media.
6. Avoid direct disk sharing with read/write access.
7. If instructed to delete e-mail messages believed to contain a virus, be sure to also delete the message from your Deleted Items or Trash folder.
8. Back up critical data and systems configurations on a regular basis and store backups in a safe place.
9. Regularly update virus protection on personally owned home computers that are used for business purposes. This includes installing recommended security patches for the operating system and other applications that are in use.

IT Department Responsibilities

The following activities are the responsibility of the Sarasota County School Board IT Department:

- Maintaining and updating these Anti-Virus Guidelines.
- Keeping the anti-virus products it provides up-to-date in terms of both virus definitions and software version in use.
- Applying any updates to the services it provides that are required to defend against threats from viruses.
- Installing anti-virus software on all Sarasota County School Board owned and installed desktop workstations, laptops, and servers.
- Taking appropriate action to contain, remove, and assist in recovery from virus infections. In order to do so, the IT Department may be required to disconnect a suspect computer from the network or disconnect an entire segment of the network.

- Performing regular anti-virus sweeps.
- Attempting to notify users of Sarasota County School Board systems of any credible virus threats via e-mail or telephone messages. Virus reports will not be acted upon until validated. Employees should not forward these or any virus warning messages in order to keep network traffic to a minimum.

Department and Individual Responsibilities

The following activities are the responsibility of Sarasota County School Board departments and employees:

- Departments must ensure that all departmentally managed computers have virus protection that is in keeping with the standards set out in these guidelines.
- Departments that allow employees to use personally-owned computers for business purposes must implement virus protection processes and procedures that are in keeping with the standards set out in these guidelines.
- All employees are responsible for taking reasonable measures to protect against virus infection.
- Employees must not attempt to either alter or disable anti-virus software installed on any computer attached to the Sarasota County School Board network without the express consent of the IT Department.

Enforcement

Any employee or student who is found to have violated this are subject to the Employee/Student Conduct Code and may be subject to disciplinary action, up to and including termination of employment/school.

APPENDIX B



Acceptable Use Policy For Computers, Networks, and Information Systems Technologies

Computer and Network Guidelines

The school district is providing access for staff and students to computers and electronic information services such as the Internet, electronic email, and calendar.

These services provide:

- District electronic mail (Outlook/Exchange) with the ability to communicate within the district,
- Global electronic mail (Outlook/Exchange) with the ability to communicate with people all over the world,
- Information and news from many sources,
- Public domain and shareware software of all types,
- Discussion groups on a wide variety of topics, and
- Access to many college and university libraries, and the Library of Congress.

The benefits for staff and students to such information access are obvious, but there are potential concerns.

These concerns include:

- Utilizing email privileges for any personal or non-professional purposes including harming the reputation of another person;
- Utilizing network resources to acquire material not considered to have educational value;
- Using network resources for destructive purposes.

District staff will continue to have access to appropriate material. However, on a global network it is impossible to control all access. The district believes that the

valuable information available on this worldwide network far outweighs the potential problems.

It is the expectation that all users of this communication system demonstrate common politeness and courtesy.

The following guidelines have been established by the School Board of Sarasota County.

If any user violates any of these provisions, his or her access to electronic information services will be terminated. Willful violations will lead to disciplinary action, and if a criminal offense is committed, the user will be prosecuted per Florida Statute 815.04.

District Network User Policies

Acceptable use of computers and electronic information services supports learning and teaching in Sarasota County.

Unacceptable use of computers and electronic information services includes:

- Sending Electronic email which harms or injures the reputation of others;
- Using network access to alter or destroy information belonging to others;
- Profanity, obscenity, or other language which may be offensive to another user;
- Copying or forwarding personal communications to others with malicious intent;
- Copying software or other copyright protected material in violation of copyright law;
- Using school board computers or the school district network for any illegal activity or for any private business purposes;
- Spreading computer "viruses" deliberately, or by importing files from unknown sources;
- Using any computer or program in a manner other than that which was intended;
- Viewing, storage, or disbursement of pornographic material;
- "Hacking" or gaining unauthorized access to district supported computer systems.

The person who has a network account is responsible at all times for its proper use.

The school district has the right to review the contents of any and all email, and all other files created or stored on school district equipment. Users are therefore

put on notice that they have no expectation of privacy when using school district computer equipment or network services.

If you have any questions about the District's guidelines or procedures, please contact your school Principal or the Department of Technology and Information Services.

These rules have been posted to all users of the district email system. By accepting the Acceptable Use Guidelines form the user agrees to these policies and procedures. The network management accepts no responsibility for harm caused directly or indirectly.

APPENDIX C



Password Guidelines

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of the School Board of Sarasota County's entire corporate network. As such, all School Board of Sarasota County employees (including contractors and vendors with access to School Board of Sarasota County systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

The purpose of this is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

The scope of this includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any School Board of Sarasota County facility, has access to the School Board of Sarasota County network, or stores any non-public School Board of Sarasota County information.

District Password Guidelines

I. General Guidelines

- All system-level passwords (e.g., root, enable, NT admin, application administration accounts, Etc.) must be changed every 45 days.
- All user-level passwords (e.g., email, web, desktop computer, etc.) will be changed at least every 60 days.
- Complex passwords will be required for all School Board of Sarasota computer logon accounts. (See section II)
- Passwords may not be repeated for twelve password changes and changes cannot be made to new passwords until after 24 hours of resetting your password.

- After 5 unsuccessful login attempts (wrong password) the account will be locked and will require a service ticket be created to have the account unlocked.
- All accounts will have a Group Policy Setting which will automatically activate screen saver and will require a password to return to normal computer usage. The screen saver will activate after 15 minutes of inactivity.
- User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- All user-level and system-level passwords must conform to the guidelines described below.
- If you will not be using your account for extended periods of time it is suggested that you at least change your password periodically (such as 10 and 11 month staff being off in the summer).

II. Password Complexity

- Does not contain the user's account name or parts of the user's full name that exceed two consecutive characters
- Must be at least eight characters in length
- Must contain characters from three of the following four categories:
 - English uppercase characters (A through Z)
 - English lowercase characters (a through z)
 - Base 10 digits (0 through 9)
 - Non-alphabetic characters (for example, !, \$, #, %)
- Complexity requirements are enforced when passwords are changed or created.

III. Password Construction Guidelines

Passwords are used for various purposes at School Board of Sarasota County. Some of the more common uses include:

User level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Since very few systems have support for one-time tokens (i.e., dynamic passwords which are only used once), everyone should be aware of how to select strong passwords.

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#\$%^&*()_+ | ~=\`{}[]:;'<>?.,/)
- Are at least fifteen alphanumeric characters long and is a passphrase (Ohmy1sturbedmyt0e).
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.

Poor, weak passwords have the following characteristics:

- The password contains less than fifteen characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
 - o Names of family, pets, friends, co-workers, fantasy characters, etc.
 - o Computer terms and names, commands, sites, companies, hardware, software.
 - o The words "School Board of Sarasota County", "SCSB" or any derivation.
 - o Birthdays and other personal information such as addresses and phone numbers.
 - o Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
 - o Any of the above spelled backwards.
 - o Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase.

For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation. NOTE: Do not use either of these examples as passwords!

IV. Password Protection Standards

Do not use the same password for School Board of Sarasota County accounts as for other non- School Board of Sarasota County access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various School Board of Sarasota County access needs. For example, select one password for internal use such as email and a separate password for external use such as web based applications.

Do not share School Board of Sarasota County passwords with anyone, including administrative assistants or secretaries.

All passwords are to be treated as sensitive, confidential School Board of Sarasota County information.

Here is a list of "don'ts":

- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an email message
- Don't reveal a password to the boss
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers while on vacation

If someone demands a password, refer them to this document or have them call the Technology Service Desk.

V. Enforcement

Any employee found to have violated this may be subject to disciplinary action, up to and including termination of employment.

APPENDIX D



Technology Service Desk

HELP

For Information Technology Support

Technology Service Desk Contact Information

Phone: x44357 or 941-861-HELP (4357)

Online: <http://help>

Email: tsd.support@sarasotacountyschools.net

Fax: 941-847-0904

Hours: 7:00am to 4:30pm, Monday-Friday

When calling or emailing the Technology Service Desk, please have the following information ready for a faster response:

- ✓ Full Name
- ✓ Location: Campus, Building, Floor & Room Number
- ✓ Phone and Extension (if applicable)
- ✓ Property Record Tag (if available)
- ✓ Best time to contact you
- ✓ Summary of your request or outage
- ✓ State if you are unable to work (urgency)