Computer Use and Security Procedure

A Guide to Computer Operating and Security for the School District of Osceola County Computer Users

Table of Contents

Computer Operating and Security

Purpose

The purpose of the SDOC Computer Use and Security Procedure:

(1) Define guidelines for our users for the proper use of computers in the district in order to minimize the risk to the computer systems and data from harm or damage due to inappropriate use or breaches of computer security

(2) Document the security policies that have been implemented to protect and secure the computer equipment and related infrastructure

This manual documents the computer users' responsibility to safeguard computer equipment and information from accidental or deliberate unauthorized access, tampering, snooping, distribution, or destruction. It sets forth what is, and is not, appropriate use of school district computers. Users may be disciplined for noncompliance with district policies and statutes, and in many cases the penalties can be severe. Should you identify an issue or situation that you are not certain how to handle, contact the administrator at your school or department.

This manual is subordinate to any collective bargaining agreement, employment contract, or other employment agreements. The SDOC may add to or change the policies at any time. It is expected that any user, technology contact or specialist, or staff responsible for computer implementations or support be familiar with these guidelines.

Any questions or suggestions for further improvements to our policies may be forwarded to the Chief Information and Technology Officer at The Osceola County School District.

Introduction

Keeping technology current is important to our effectiveness and efficiency of operations, and provides unprecedented opportunity for both students and employees to succeed. In that same vein, it puts us at considerable risk. Implementing new technologies is expensive, time consuming, and without established policies and practices in place, could lead to disaster.

A well-trained work force properly educated in computer operating procedures, and computer user security matters, will have the best chance of minimizing interruptions due to inappropriate, negligent, or unethical use of computers and related infrastructure. To meet this need, a number of resources are made available to the students and staff of the district.

1. This security procedure
2. Security Awareness training required by all employees
3. Network Acceptable Use policy
4. Regular Tech Contact training and meetings
5. Knowledge base articles
6. The Information Services Standard Operating Procedures

Employee Computer Operating And Security Guidelines

Computer Users

Users are responsible for the appropriate use of SDOC computers and communications resources and for taking reasonable precautions to secure the information and equipment entrusted to them. Employees are responsible for reporting inappropriate use of SDOC computers, breaches of computer security, and assisting in resolving such matters. Users are responsible for adhering to policies and practices as described herein, and in other policies and procedures to ensure that computer and communication resources are used appropriately and that reasonable measures are taken to prevent loss or damage of computer information and equipment.

Unauthorized Access

Unauthorized access of computers (hardware and software) and communications resources (e.g. Internet access, web servers, e-mail) is prohibited. Unauthorized access to data files and automated systems is prohibited. Within Osceola County Schools this means access without appropriate specific authorization is prohibited.

In addition, any form of tampering, including snooping and hacking, to gain access to computers is a violation of SDOC policy and carries serious consequences. Employees are required to turn their computer off (or secure their workstation) at the end of the day and when not in use for an extended period of time. This will help prevent computer security breaches, and damage due to power surges. In addition, computer users must take other reasonable precautions to prevent unauthorized access of school district computers.

During work hour, if an employee walks away from their desk they should “lock” their computer to secure it from unauthorized use. On a PC this can be done by simultaneously pressing the Ctrl + Alt + Delete keys and selecting “Lock computer” or by simultaneously pressing the Windows key (next to the Alt key) and the letter “L”

Computer Sabotage

Destruction, theft, alteration, or any other form of sabotage of SDOC computers, programs, files, or data is prohibited and will be investigated and prosecuted to the fullest extent of the law.

Passwords

The use of a user ID and password combination is supposed to securely identify and authenticate users for system and data access. Without the use of strong passwords that are constructed according to a proper policy, the security that passwords supposedly supply quickly fails.

Password Selection and Protection

Select difficult passwords. Change them regularly, and protect them from snoopers. A lot of damage can be done if someone gets your password. Users will be held accountable for password selection and protection. SDOC requires that users change their passwords to the IBM iSeries system (TERMS) and Active Directory every 90 days. These systems also enforce certain password rules which ensure that your password is not a simple one.

Do not share your password with anyone. Do not write it down where someone can find it, do not send it over the Internet, Intranet, e-mail, dial-up modem, or any other communication line.

All users (whether employees, volunteers, parents, or consultants) of networked information systems with data access privileges must be properly authorized and provided an individual password. This involves both specific authorization and access levels appropriate to job duties and legitimate educational interests.

Password Cracking

It is not uncommon for employees to try to figure out a friend's, or associate's password, just to see if they can. However, the same employee would never steal the key and go through your desk drawer looking at everything and anything private and confidential. Yet, this is just what happens when passwords are cracked. Stay away from such activity. It is a serious violation of SDOC procedure.

Easy to Remember and Hard to Crack

Another concern is forgetting your password. Getting into your computer when you have forgotten the password is, in some cases, very difficult. A good method to help you remember your password is to select passwords that are unique to you and try to use it at least once every day.

In general the following are good tips for creating strong passwords:

- Has both upper and lower case letters
- Has digits and/or punctuation characters as well as letters
- Is easy to remember, so they do not have to be written down
- Is seven or eight characters long
- Do use a password which you can type quickly, so someone else cannot look over your shoulder
- Do not use your employee id number as a password
- Do not use all or part of your login name, your name, your spouse's name, children's or pet's name, or any other names commonly known to others
- Do not use a word pertaining to SDOC, your work, or an activity that you participate in or follow that is commonly known
- Do not use words that are derogatory, offensive, or defamatory

In addition, some systems may enforce additional password rules which ensure the security of that system.

Password Resets

Several passwords can be securely accessed through the SDOC Employee Portal. You may retrieve your intranet password on the portal. You may reset your TERMS password if you have a TERMS account. Other password issues can be handled by calling the Help Desk.

Snooping

Snooping into SDOC computer systems is a serious violation of SDOC procedure. If you have no business being there, don't go there. If you accidentally identify a new way to access information, report it to management. Watching other users enter information and looking at computer disks that do not belong to you are prohibited. Obtaining or trying to obtain other users' passwords or using programs that compromise security in any way, are violations of SDOC procedure and are likely violations of state and federal statutes. If you observe someone snooping, report it to management.

Hackers

It takes a concerted effort by all employees to maintain secure computer systems.

Hackers are working hard to break into computer systems. They alter and delete files, and cause other havoc for fun or profit. Hackers frequently penetrate computer systems by calling unsuspecting employees representing themselves as a new employee, an SDOC administrator, or another trusted individual. Through a variety of probing questions, they obtain the information necessary for their hacker programs to do their work.

Never give any information about computer systems over the telephone or in any other way, with the exception of calling the Help Desk. If someone requests such information get their name and phone number and tell them you will get right back to them. Report the incident immediately to your school site or department management and to the district's Technology & Information Services Office (407-870-4050). Without your help the SDOC has little chance of protecting the SDOC's computer systems.

Using hacker programs and trying to access computer systems using hacker techniques is prohibited. Trying to hack into third party computer systems using SDOC computers is prohibited and will be reported to the local authorities. If you are caught hacking, it is a serious offense. If you identify vulnerability in the SDOC's computer security system, report it to management.

Viruses, Worms and Trojan horses

Several methods are used to keep viruses off our computers and network. All email is scanned for viruses, both incoming and outgoing. The school district has installed an anti-virus program on all SDOC computers. Tampering or disabling the anti-virus program is prohibited.

It is critical that users make certain that data and software installed on SDOC computers are free of viruses. Data and software that have been exposed to any computer, other than SDOC computers, must be scanned before installation. This includes downloads from the Internet and other sources of data that may be contaminated. Viruses can result in significant damage and lost productivity. If you are uncertain whether data or software needs to be scanned before installation, contact your local Technology Contact or the Help Desk.

Use of virus, worm, or Trojan horse programs is prohibited. If you identify a virus, worm, or Trojan horse, or what you suspect to be one, do not try to fix the problem. Immediately turn your computer off, make notes as to what you observed, and contact the school technology contact or Help Desk. Do not open attachments from unknown or suspicious sources. The school district has installed an Anti-Virus program on all SDOC computers.

The principal concern is stopping the contamination before additional damage is done. Viruses are designed to easily hop from application to application, contaminate a computer disk and access another computer. They easily travel down phone, cable, ISDN, or other communication lines, infect e-mail, data and files, and find their way to other computer systems. The key to containment is limiting the reach of the contamination. Deleting messages or turning off your computer and consulting your site technology contact to assist you is advised.

Confidentiality

General

All computer information is considered confidential unless you have received permission to use it. Accessing or attempting to access confidential data is strictly prohibited. Confidential information should only be used for its intended purpose. Accessibility is not to be confused with authorization. In other words, even though you may be able to access and read or print-out information on your computer or on the network, you are responsible for accessing or using that information in which you have “direct and legitimate educational interest.”

Handling Confidential Information

Confidential information stored on computers is typically more difficult to manage then traditional paper documents that are sealed in an envelope and locked in a filing cabinet clearly labeled CONFIDENTIAL. As such, it is important that users take extra care with confidential information stored on computers.

The following are ***inappropriate*** under normal circumstances when dealing with confidential information:

- ♦ Printing to a printer in an unsecured area where documents may be read by others
- ♦ Leaving your computer unattended while logged on while confidential information is in view
- ♦ Leaving computer media (disks, CD’s, USB drives, etc.) with confidential data unattended in easy to access places.
- ♦ Sending confidential information over non-secured Internet or other network connections. This includes posting of grades for parental or student access. Appropriate security procedures are essential. This typically requires user authentication and authorization, encryption or protection of the transmission packets, and access records and controls. Contact your site or department technology contact, departmental management, or information systems/technology services management for guidance on what constitutes acceptable security steps.
- ♦ Remember that where you store confidential data files (including back-ups) must be in a secure location or reasonably secure from unauthorized users.

If you observe a document at a shared printer, or any other location, do not read it without permission.

Encryption

If you need to send confidential or proprietary information over the Internet, or other public communication lines, you must ensure that it is over a secure, encrypted connection. Website that are secure start with and "https" address where the "s" indicates a secure connection. Other methods exist for sending data securely. Contact Information Services or Technology Services for help.

Note that when sending email messages between other FirstCLass users our network, the email message is secure and encrypted. However, when sending and receiving email to or from others people not using FirstClass, the message is not secure and not encrypted.

Physical Security

Locks

Physical security is vital to protecting your computer and computer information from loss and damage. Store media such as CD's, disks and USB drives containing sensitive data in a locked drawer or cabinet. Turn off your computer when it is not in use for an extended period of time. Lock the door to your office if you have one. Take a few minutes to practice good physical security.

Laptops

There is no sure way to secure laptops. However, there are many sensible cost-effective measures that can help reduce the risk of loss or damage. The following are required when taking laptops off SDOC property:

- If possible, do not leave your laptop in your car or other vehicle
- Report lost or stolen computers immediately
- All important files must be backed-up and back-up disks must be stored in a separate physical location from the computer
- Use reasonable precautions to safeguard the laptop against accidental damage
- When traveling, laptops must be in sight at all times or physically secured
- Always store laptops in a concealing carrying case
- Personal laptops are not authorized for use on the SDOC network

Off-Site Computers

Off-site users must take additional precautions to safeguard computer information and equipment, including but not limited to:

♦ Safeguarding the computer and information from theft or damage
♦ Prohibiting access to the computer (including family, friends, associates, and others) for any purpose without management authorization
♦ Adhering to all computer policies and practices of the SDOC for on-site users

Administrative Matters

Back-up

All SDOC computer users have a network drive called the "U" drive where they can save important documents and files. The "U" drive is the preferred place to store your important documents and other data since it resides on the network drives and is secured and backed up regularly. In addition, each department has a network drive called the "Q" drive which also resides on the network drives and is backed up regularly.

If for some reason you do not have access to your "U" or "Q" drive, you will need to consider backing up the data some other way. Backing up files is vital to productivity and safeguarding data against unwanted intrusions. Important files should be backed-up daily. Decisions about what to back up, and how often to back-up should be considered with one simple thought in mind. How much productivity would be lost if your computer were stolen or your data gets corrupted? So much work is done in a single day that in most cases it is irresponsible to not take a few minutes to back-up essential data.

All backed-up files should be stored on a secure computer disk or tape other than the one containing the original data. The back-up disk or tape should be stored on site, preferably in a fire proof cabinet.

Copyright Infringement

The SDOC does not own computer software, but rather licenses the right to use software. Accordingly, SDOC licensed software may only be reproduced by authorized SDOC officials in accordance with the terms of the software licensing agreements. Unauthorized copying, redistributing, and republishing of copyrighted or proprietary material are strictly prohibited. Copyright laws apply on the Internet as well. Copyright infringement is serious business and the SDOC strictly prohibits any such activity. If you have questions about copyright infringement, discuss it with management.

Shareware and free software often have licensing and use restrictions and should not be copied or forwarded to others. Typically, if you continue to use shareware you must send in a “donation,” often of a specified amount. If you neglect to do so, you may have committed copyright infringement. If you provide the program to a friend, you may have violated copyright law. It is not unusual for “free” software to contain a virus.

Each user is responsible for the software he or she uses. If you are not sure if your school or department has licenses for the software you are using, ask. Your school or department should have a purchase order (or an explicit reference for a purchase order or licensing agreement if the software was provided for outside the school or department) reflecting payment for the number of licensed products currently in use.

Harassment, Threats and Discrimination

It is SDOC procedure, and the law, that employees are able to work free of unlawful harassment, threats, and discrimination. Unlawful harassment is physical or verbal behavior directed towards an individual due to their race, age, marital status, gender, disability, religion, sexual orientation, or nationality for the purpose of interfering with an individual’s work performance, or creating an intimidating or hostile work environment.

It is not uncommon for employees to receive files, data, pictures, games, jokes, etc., that may be considered offensive by some. The computer is possibly the easiest tool for obtaining, storing, sharing, and disseminating to large audiences such material and viewpoints. Be cautious and careful when sharing items that may be disruptive or inappropriate. It is inappropriate to use SDOC computers to share your personal views about religion, politics, sexuality, or any other subject of a personal nature that could be considered offensive to others within or outside the SDOC. SDOC computers are not vehicles to express free speech. Do this on your own time, away from the SDOC, using your own resources.

Computers provide a huge potential for unlawful harassment. Users often think their communications are private and trashed or deleted files are gone forever. However, deleted files are often easily recovered and information on SDOC computers is not necessarily private. Users often feel comfortable writing and storing files within the confines of their “personal” computer, and sharing personal views on a wide range of non-business subjects. Remember, whatever you transmit is a permanent record to the receiver. It can, at some future date, be taken out of context and used against you and the SDOC. Be very careful about “broadcasts” to groups when you copy, forward, or reply to messages. These may include more than your intended audience.

Accidents, Mistakes and Spills

It is not hackers, snoopers, viruses, worms, or Trojan horses that cause the most damage to computers and information. It is, by far and away, us, the computer users. According to current research, most data loss and damage to computers is done by authorized users. Mistakes and accidents represent the biggest cost when it comes to computer information loss. We have all done it, deleted a file that we just spent hours creating, spilled coffee on the keyboard, or dropped the laptop on the floor.

“*An ounce of prevention is worth a pound of cure”* is a very appropriate cliché for computer operations. Take a few seconds to read the computer screen before you delete, save, or transmit files. In addition, users need to take reasonable precautions with respect to computer operations, maintenance, handling, and transportation. It is not our intention to prohibit coffee at your desk. However, when placing liquids, and other food items on your desk, please be careful.

Unauthorized Changes to SDOC Computers

Installing software and making changes to computer hardware, software, system configuration, and the like always carry with it the possibility of disrupting or replacing essential applications. If you are not sure about an upgrade, replacement, or new installation, contact your site technology contact.

The SDOC’s computer systems have been designed and documented to prevent loss of data, and provide an audit trail for correcting problems. Unauthorized changes to computer systems ultimately result in lost productivity. Such changes often require a computer technician to fix both the original problem and the problem caused by the would-be computer technician. Poor documentation of the procedures performed and the order in which they were completed further complicate unauthorized changes to computer systems.

The following are just a few examples of changes to computers that can result in operating problems:

- Installation of commercial software, shareware, and free software. Some software requires an upgrade of computer hardware, the operating system, or both for the program to operate properly. Some programs are simply not written well, and can cause problems with the computer
- Installation of some programs changes the computer’s system configuration, which can result in problems with your computer

- Data used on home computers may become infected with a virus and contaminate your computer and other SDOC computers
- Screen savers can often interfere with certain programs or program operations. It is generally better to avoid add-on screen savers if you are running a variety of programs on your desktop.

The list of potential problems goes on and on. Accordingly, get approval from management before making any changes to SDOC computers.

Purchases of Computer Software and Equipment

Purchases of computer software and equipment are prohibited without approval from departmental management and SDOC. All computer software and hardware purchases should follow district guidelines, established quality requirements to ensure cost-effective purchases and be compatible with other SDOC computer software and equipment.

The SDOC has established guidelines for schools and departments when the purchase of new software programs is considered. It is the responsibility of the personnel at the school level or district department to verify that the same or a similar program is not already in use by referring to the Approved Software list, found on the intranet under the Media & Instructional Technology Department. Guidelines for the selection of software can also be found at their site. Any software over $500 must be approved by the Software Evaluation Committee. This application process is necessary to ensure adequate technical support to properly run the software on existing computer systems and networks. Specific criteria include the cost of the program, and whether it is web-based or requires a file server. Before submitting a request to purchase software, each portion of the application must be completed, and references are required. The application forms can be printed from the MIT intranet site as well.

Disposal of SDOC Data

Purge files that no longer have a practical use on a periodic basis. Old computer files utilize disk space and often represent a potential hazard to you and the SDOC. Delete old personnel evaluations, compensation information, sales and financial information, customer information, and vendor data. Electronic versions of official correspondence and records fall under the same guidelines and rules as “hardcopy” records, including records retention and destruction guidelines. Please consult the SDOC Records Retention Handbook if you have questions regarding records destruction.

A word of caution, permanently removing a file from your computer is something you need to consider carefully before taking action. Recreating a file you did not intend to delete is tedious and time consuming. Although the file probably exists on back-up, it is not always practical for the site/department Technology Contact to expend the resources necessary to find the file. The LAN backup is principally designed to recover the entire system, not a single file.

Personal Use of Computers

Incidental and occasional personal use of SDOC computers is permitted for reasonable activities that do not need substantial computer hard disk space or other computer equipment. As a general rule, if you would be uncomfortable asking for permission, it is probably not an appropriate use of SDOC computers. Prohibited activities include, but are not limited to, computer games, personal software and hardware, writing your autobiography. Use of school district equipment for personal business is prohibited. Using SDOC computers to store or transmit inappropriate jokes, junk mail, chain letters, or to solicit for commercial, religious, charitable, or political causes is prohibited. If you are uncertain about a specific activity, ask your supervisor.

Many software games are illegally copied and often contain viruses. Such programs represent a potential liability to you and the SDOC. Proof of ownership and management authorization for use is required for all software on SDOC computers. Coming to work with a computer game, on an unlabeled disk, can result in system damage and extensive recovery costs. Playing games on work time or non-business use of computers during work time must be within the parameters of good judgment and site or department rules.

Proprietary Information

SDOC data, databases, programs, and other proprietary information represent SDOC assets and can only be used for authorized SDOC business. Use of SDOC assets for personal gain or benefit is prohibited. Sharing SDOC proprietary information with SDOC personnel, or third parties, is prohibited.

Reporting Violations

Employees are required to report violations or suspected violations of computer procedure. Activities that should immediately be reported to management include, but are not limited to:

- Attempts to circumvent established computer security systems
- Use, or suspected use, of virus, Trojan horse, or hacker programs
- Obtaining, or trying to obtain, another user’s password

- Using the computer to make harassing or defamatory comments or to, in any way, create a hostile work environment
- Using the computer to communicate inappropriate messages or jokes that may be considered offensive by others
- Illegal activity of any kind
- Trying to damage the SDOC, or an employee of the SDOC, in any way

Computer procedure violations will be investigated. Noncompliance with the SDOC's employee computer procedure may result in discipline up to, and including, termination. Employees that report violations or suspected violations of SDOC procedure will be protected from termination, discrimination, harassment, and any other form of retaliation. Hackers, snoopers, password stealers, virus installers, data erasers, and anyone involved in such activity will be disciplined.

If you identify computer security vulnerability, you are required to report it immediately. Call the Help Desk (407-870-4037) or Technology Services (407-870-4050). Options and steps that can be taken to minimize exposure, damage, or tracing of the problem source, are more effective the sooner these are implemented.

Termination of Employment

All information on user computers is considered SDOC property. Deleting, altering, or sharing confidential, proprietary, or any other information upon termination requires management authorization. The computer you have been entrusted with must be returned with your password, identification code, and any other appropriate information necessary for the SDOC to continue using the computer, and information, uninterrupted.

The following activity is prohibited upon termination, and will be prosecuted to the fullest extent of the law:

- Accessing SDOC computers
- Providing third parties, or anyone else, access to SDOC computers
- Taking computer files, data, programs, or computer equipment

Privacy

Monitoring Computer Communications and Systems

Many people think data stored on computers, transmission of data between individuals on dial-up modem lines, communications on the Internet, and e-mail are private and in most cases they are. However, the SDOC reserves the right, without prior notice, to access, disclose, use, or remove both business and personal computer communications and information and will do so for legitimate business purposes.

Random audits to verify that SDOC computers are clear of viruses and used in accordance with SDOC procedure may be performed. The SDOC will investigate complaints about inappropriate images on computers, inappropriate e-mail, or other inappropriate conduct. The SDOC may monitor Internet activity to see what sites are frequented, duration of time spent, files downloaded, and information exchanged. Again, computer systems and information are SDOC property and should be used principally for business purposes.

It is management's fiduciary responsibility to:

- ♦ Establish and enforce procedure to help prevent the violation of personal rights and illegal acts
- ♦ Reduce the risk of liability and business interruption to the SDOC
- ♦ Maintain a professional work environment where computer abuse will not be tolerated

Lawsuits and Subpoenas

SDOC computers, like any other SDOC property, are subject to subpoenas. This means that prosecutors and plaintiffs' attorneys may access SDOC computers, and look at information to gather evidence in a complaint. It is not difficult to imagine how easy it would be to find embarrassing and possibly incriminating information on SDOC computers. For attorneys skilled in electronic discovery, the wealth of information is immense.

It is not management's intention to suggest that you remove any information from your computer, now or at any other time or to in any way hinder an investigation of any kind. Quite the contrary, management prohibits such activity. Management's intention is to ensure that users conduct their work to the highest ethical standard with the knowledge that computer information (even deleted files) can be used against you and the SDOC in a legal proceeding.

External Communications

Third Parties

The same standards of decorum, respect, and professionalism that guide us in the office environment, apply to computer communications with third parties. Important, confidential, and proprietary information is stored on SDOC computer systems. Accordingly, only SDOC personnel are allowed access to the SDOC's computer systems without written authorization from management. Management must approve computer data and other information received by, or provided to, third parties. Please keep in mind that third parties may have a legitimate business need, duty, legal right, or obligation to access, disclose, or use information transmitted.

Dangers of the Internet

An unauthorized hot link is a program installed on a legitimate web site by an unauthorized individual. The program changes, or adds to, the path of information transmitted. As such, the user may unknowingly send information to a location not authorized by the web site administrator as well as the intended destination.

Copyright laws can be enforced on the Internet. Viruses can be downloaded from the Internet. Inappropriate web sites, images, and communications exist on the Internet. Competitors exist on the Internet. Hackers exist on the Internet. As such, users must follow established computer operating policies and practices to reduce the opportunity for security breaches, and inappropriate or illegal activity resulting from connecting to the Internet.

Internet Connections

Internet connections are authorized for specific business needs only. Connection to the Internet without management authorization is prohibited. The following activities are prohibited without management authorization:

- Downloading information of any kind, including data, files, programs, pictures, screen savers, and attachments
- Exploring the Internet for fun or profit
- Establishing communications with third parties
- Research for personal or business purposes
- Forwarding or transmitting information to third parties or employees
- Copying programs, files, and data
- Transmitting important, confidential, or proprietary information
- Speaking on behalf of the SDOC

Individuals that have received management approval to transmit information on the Internet should understand that such transmissions are identifiable and attributable to the SDOC. Disclaimers such as "*The opinions expressed do not necessarily represent those of the SDOC,*" while a good idea, do not necessarily relieve the SDOC of liability. The Internet should be considered a public forum for all transmissions. All communications on the Internet provide an opportunity for a permanent record and can be edited and retransmitted. Accordingly, maintain a professional decorum in all communications and transmissions.

The following actions are prohibited under any circumstances:

- ♦ Portraying yourself as someone other than who you are or the SDOC you represent
- ♦ Accessing inappropriate web sites, data, pictures, jokes, files, and games
- ♦ Inappropriate chatting, e-mail, monitoring, or viewing
- ♦ Harassing, discriminating, or in any way making defamatory comments
- ♦ Transmitting junk mail, chain letters, or soliciting for commercial, religious, charitable, or political causes
- ♦ Gambling or any other activity that is illegal, violates SDOC procedure, or is contrary to the SDOC's interests

Business Reputations

Please keep in mind, a statement or posting of information on the Internet can cause serious damage, because information can be quickly and effectively disseminated. The SDOC, and the law, can and will hold you responsible for offensive, discriminatory, and defamatory statements, or any other illegal activity.

Email

Electronic Communications

The same standards of decorum, respect, and professionalism that guide us in our face-to-face interactions apply to the use of email. The SDOC Network Acceptable Use Policy outlines what is expected of the user regarding the use of email.

Incidental or occasional use of email for personal reasons is permitted. However, only SDOC personnel are allowed access to the SDOC email system. The following email activity is prohibited:

- ♦ Accessing, or trying to access, another user's email account
- ♦ Obtaining, or distributing, another user's email account
- ♦ Using email to harass, discriminate, or make defamatory comments
- ♦ Using email to make off-color jokes, or send inappropriate email to third parties or other SDOC employees.

- Transmitting SDOC records within, or outside, the SDOC without authorization
- Transmitting junk mail, chain letters, or soliciting for commercial, religious, charitable, or political causes.

Employees are required to report inappropriate use of email.

As a general rule: If the use is consistent with the educational mission of the school system and involves content appropriate for the school context generally; if the use occurs during break or lunch times and is acceptable to the supervisor; and if the use does not impact other users on the system or restrict needed shared system resources (for example, sending an email message may be acceptable; however downloading or viewing a multi-media video or soundtrack during a time when this may consume bandwidth and preclude or slow other school business or instructional activity is not acceptable). It is always advisable to confirm with your administrator or supervisor any uses which could be construed as misuse of school system property.

Dangers and Pitfalls of Email

Appropriate email etiquette is essential to maintaining a productive and professional work environment. Comments that might be made at parties, in elevators, and on the telephone are now done via email. However, email does not disappear into thin air. It can be widely, easily, and quickly disseminated. Email can be edited, forwarded, distributed, and filed for later use, possibly at the most inopportune time. If you would not put it in a memorandum on SDOC letterhead, do not say it with email!

Mark Grossman, author of Computer Law Tip of the Week and columnist for the South Florida Daily Business Review, believes in four basic rules for using email:

- *Never, ever give bad news by email. Bad news always deserves a real human voice, whether over the phone or in person*
- *Never use email to criticize people. It stings much more in writing and does not heal with time. All day long, the recipient gets to reopen the email and feel bad all over again. Critical email inevitably eats at the craw of the recipient*
- *Never discuss personal issues over the office email system. It's truly bad office etiquette. CC's being what they are; you may just see that personal email posted on the lunchroom bulletin board. (Hint: Any email that starts with "Oh, honey" is probably a personal email that should not be in the office computer system.)*
- *If there is even the slightest possibility that what you are going to say could be taken wrong, don't use email to say it*

Follow Mr. Grossman's four basic rules of email. Keep in mind, email is not the only form of communication (although at times it may seem that way). If you have something confidential or sensitive to say, there are better ways to communicate your message. It is still good practice to use the phone, or stop by someone's office and talk face-to-face.

Virus control

The most common means of virus attack is via-email. It is important that users must not forward or open unsolicited attachments or attachments from unknown sources. The disruption and denial of services caused by viruses is an increasingly costly and critical impact to mission critical data and communications systems. SDOC makes every effort to screen inbound and outbound viruses out of our email, and places restrictions on the ability to open certain file types that are known to be used in virus attacks.

In addition to being skeptical about attachments, the same caution holds true for web links sent in unsolicited emails. Following a web link may not necessarily lead you where the link appears to go, and can result at best in verifying your email address to a spammer, and at worst, tricking you into revealing personal information that can be used for identity theft.

Regardless of all best efforts, any email message you receive or send which includes an attachment might cause problems. Therefore, try and follow the rules below;

Receiving Email with an Attachment: **- do not forward or open unsolicited attachments or attachments from unknown sources.**

DON'T TOUCH THE ATTACHMENT. Don't open it, don't view it, and don't save it to the disk.

1. Contact the person who sent it and verify they actually sent it to you. If you do not know the sender, it is more likely to be a virus.

2. Ask them what it is, specifically.

3. If you're at all unsure about it, contact the person you turn to if your computer is acting up. If you're in an office, contact your Administrator or Technology Contact. If you're at home, contact your ISP (Internet Service provider). DO NOT SEND THEM A COPY OF THE ATTACHMENT, describe it to them and then wait until they ask you for it.

Sending Email with an Attachment: - *remember, you could be sending them a virus!*

1. Describe what the attachment is and why you are sending it. Remember, viruses can do this too, so try and include something unique in this message so the recipient will know it's from you and not some automated virus.

2. Avoid sending messages with attachments that contain executable code (codes that run things), like Word documents with macros. You can use rich text Format, or RTF, instead of the standard DOC format. RTF will keep your formatting, but won't include any macros. There is, however, a couple of viruses out there that will fool Word when you save as RTF, so while you cannot completely trust RTF files it is still good practice. This may avoid the embarrassment of you sending them a virus if you are already infected.

3. On your home computer, run an Anti-virus product and set it to update frequently (at least once every 24 hours is recommended), but don't rely on it to completely protect you. Remember, they can only detect what they already know about. Specifically scan any file you are going to include as an attachment in an email before you send it to someone else.

Always err on the side of using email safely.

This problem is not going away. You need to think of this like you think of locking your doors at night or riding a bike on a busy street. There are safe ways and unsafe ways, be smart, ask questions, and think before you click on things.

Forwarding Information

Email makes attaching files and forwarding data a snap. However, the damage from forwarding something to the wrong person may be serious. Please take a minute to think through the appropriateness of all the parties you are forwarding. If you receive an email (particularly email with an attachment) and intend to forward it to others, consider the following:

- ♦ Is any of the information unnecessary or inappropriate for any individual?
- ♦ Would the author take exception to, or be embarrassed by, your forwarding the information? (A good rule of thumb is to copy the author.)
- ♦ Might the information be received negatively?
- ♦ Might the information be misunderstood?
- ♦ Is the receiver likely to forward the information to individuals that should not have, or do not need, the information?
- ♦ Do the attachments have viruses? Email attachments from unrecognized or unknown sources must not be opened or forwarded due to the risk of viruses

If the answer to any of these questions is yes, do not forward the information. Edit it, or create a new file. A bad decision can result in misunderstanding, hurt feelings, and added work.

Student Information in email

The exchange of student information is regulated by state and federal law, and therefore must be treated in a careful manner when using email. It is illegal to send identifiable student information to parties that have no legitimate educational interest in the student.

It is SDOC policy that student information may be exchanged through email with other SDOC email users, since that information stays within our network. Because email that is sent outside our network to internet addresses can potentially be intercepted or sent to mistaken addresses, such email must NOT contain identifiable student information. For example, a student's initials may be substituted for an identifiable name. This restriction applies to all internet mail, parents and outside counseling agencies included.

Spam

Sending unsolicited messages or files to individuals, groups, or organizations that you do not have a prior relationship with is prohibited without written authorization from your supervisor. Sending messages or files with the intent to cause harm or damage to the intended receiver is a violation of SDOC policy and will be prosecuted to the full extent of the law.

SDOC uses a high-performance spam filter to reduce the amount of spam coming in to our email system. Of over 300,000 messages received daily, only 10% are allowed to reach user's mailboxes. Offensive spam that does manage to reach user's mailboxes should be discarded, or reported to the Help Desk, depending on the severity of the message.

Passwords

A strong password is essential for email security. Because the "default" password assigned to new accounts is widely known, it is essential that your email password be changed as soon as you first log in to your new account, and at least every 90 days thereafter. Choose a password that is difficult to guess and contains numbers and special characters, similar to your active directory password.

If your email password is known to others, they can log into your account and impersonate you. You only need to imagine the potential consequences that could result from such actions to remind yourself to keep your password secure.

Mobile Devices

Because Florida Public Record laws consider email documents to be public record, it is important to keep this in consideration when using mobile devices such as Cellphones, Smartphones, and PDA devices to send email messages that contain content regarding SDOC business.

At the present time, forwarding of SDOC email messages to personal mobile devices or personal email accounts is prohibited without the express permission of the Director of Information Services. Additionally, using other email clients and the POP email protocol to access our email server is prohibited.

Our email system is accessible using any web browser, or the same client software used at the District is freely available for use on home computers. For mobile devices, there is client software available for some products, or a web page designed for portable devices is available (http://mobilemail.osceola.k12.fl.us). There is no need to forward SDOC business email to other mail servers.

As the options for mobile device communication with our email system evolve, the Information Services Department will make those options available to our users as soon as they can be practically applied.

Archiving

SDOC email is archived only for the following groups: Board Members, The Superintendent, District level Administrators, and Principals. Messages sent to members of these groups, whether from internal or external sources, as well as all their outgoing mail is stored on an archive server with a retention period of seven years.

Email expiration

Email messages on the SDOC email system automatically expire at the end of 90 days in the user's inbox. At that time they are transferred to the Trash Can for another 7 days. After that time, they are completely removed from the email server. If a user needs to retain an email longer than 90 days, they should print it and file it, or move it to a folder in their email inbox.

Account Privacy

The SDOC Network Acceptable Use Policy states that minor personal use of email is permitted. Because the email system is used to conduct the business of the school district, the privacy of the account is not guaranteed, and the contents of an email account can be accessed at any time necessary by authorized administrators. In addition, the contents of our mailboxes are subject to Public Record requests, as well as subpoena requests from law enforcement agencies.

It is highly suggested that employees use their own personal email accounts for personal messaging.

More Information

There are many sources of help and information regarding our email system to assist you in your daily tasks.

- Use the F1 key to bring up help text regarding the current window you are using, or use Help > Contents for all help screens.
- Contact your school or department Tech Contact for personal assistance.
- Call or email our Help Desk (ext. 67000) for emergency assistance.
- Take an inservice course offered by the Media and Instructional Technology Department.
- View the video tutorials offered on our email website at http://fc.osceola.k12.fl.us/videos/

SDOC wants you to have a rewarding experience using email. Please use it responsibly, and provide constructive feedback you feel would improve the system for all of our users.

Intranet

The SDOC Intranet can provide significant efficiencies and it makes dissemination of information easy and cost-effective.

Data, programs, and other information are updated regularly on the Intranet. As such, it is your responsibility to ascertain that information you are working with is current.

The same standards of decorum, respect, and professionalism that guide us in the office environment apply to the use of the Intranet. Important, confidential, and proprietary information is stored on the Intranet. Accordingly, only SDOC personnel are allowed access to the Intranet without written authorization from management. All SDOC policies apply to use of the Intranet. The following activities are prohibited without management authorization:

- Installation of a web site, page, or any other information
- Installation of business or personal software on the Intranet
- Exceeding authorized access of Intranet programs, data, and files
- Assisting anyone outside the SDOC in obtaining access to the Intranet
- Making any changes to the Intranet hardware or software

Local Area Network

All important, confidential, or proprietary information must be stored on the LAN. Storing information on your desktop computer introduces security risks and requires extraordinary care to ensure security and privacy. Typically, the LAN is equipped with electronic and physical security. Activity on the network is monitored for tampering and other security breaches. Maintenance and back-up are performed on the LAN daily and programs and other information are updated. Use the LAN! It is safe, effective, and reliable. Because important, confidential, and proprietary information is stored on the LAN, only SDOC employees are allowed access. All SDOC policies apply to the LAN. The following activities are prohibited without management authorization:

- Installation of business or personal software on the LAN
- Making any changes to the LAN hardware or software
- Accessing LAN programs, data, and files without authorization or exceeding authorization
- Assisting anyone within, or outside, the SDOC in obtaining access to the LAN

Receipt of
Employee Computer Operating
And Security Procedure

I have received and read SDOC's Computer Use and Security Procedure. I understand that I am responsible for adhering to the policies and practices described therein. I understand that these policies may be added to, or changed by the SDOC at any time. It is my responsibility to bring any questions I have about the Computer User and Security Procedure to my supervisor. I further understand that it is my responsibility to report any violations of this procedure that I witness, or become aware of, during the course of my employment.

____________________________ ________________
Employee Signature Date

____
Employee Name (Please Print)

Glossary of Terms

Computer Information

Data, software, files, and any other information stored on SDOC computers and systems.

Encryption

The process of turning plain text into cipher text by applying an algorithm that rearranges or changes its input into something unrecognizable.

Firewall

A specifically configured system that serves as a secure gateway between an outside network (e.g., the Internet), and the organization's internal networks.

Hacker

Slang, an individual intensely absorbed with and/or extremely knowledgeable about computer hardware and software. Also used to describe those who break into and corrupt computer systems. (Hacker is used here to describe those who break into and corrupt computer systems.)

Hot Links

A connection made between application programs so that when changes are made to the data in one file, the changes appear instantly in another.

Intranet

A local area network which may not be connected to the Internet, but which has some similar functions. Some organizations set up World Wide Web servers on their own internal networks so employees have access to the organization's Web documents.

Internet

The mother of all networks. A group of networks connected via routers.

ISDN

Integrated Services Digital Network. Digital telecommunications lines that can transmit both voice and digital network services, and are much faster than the highest speed modems.

LAN
A set of connections between computers that provides the basis for electrical transmissions of information, generally within a small geographical location to serve a single organization.

SDOC

School District of Osceola County School Board or Osceola County Schools.

Login
A start-up file stored in the user's directory. This file is used to execute commands that should only be executed at login time, such as establishing the terminal type and starting windows systems.

Modem
Short for modulator-demodulator. A hardware device that allows two computers to communicate over ordinary telephone lines.

RAM
Random Access Memory. The working memory of the computer. RAM is the memory used for storing data temporarily while working on it, running applications programs, etc. "Random Access" refers to the fact that any area of RAM can be accessed directly and immediately.

Server
A computer or device that administers network functions and applications.

Trojan horse
A program that masquerades as something it is not, usually for the purpose of breaking into an account or exceeding commands with another user's privileges.

Virus
A set of instructions that can reside in software; and can be used to destroy other files or perform other tasks with another user's privileges.

Web Site
A server computer that makes documents available on the World Wide Web. Each web site is identified by a host name.

Worm
A program that propagates by replicating itself on each host in a network, with the purpose of breaking into systems.

Appendix

Who You Can Contact if Your Computer System is Hacked Into

Any security breach relating to passwords or electronic data files or systems must be reported immediately (or as soon as emergencies permit) to Information Services 407-870-4045 or Technology Services 407-870-4050. It is increasingly the case, particularly in the electronic medium that "hacks" or "breeches" are widespread; that logs or records are more complete/detailed as these data are more current; and that appropriate legal and procedural steps are taken as consistently as possible. Typically, our effectiveness in minimizing damages due to a security breech and our ability to trace security problems is greatly improved where appropriate communications have occurred quickly.

For further information regarding computer security violations and what to do, contact the **CERT Coordination Center (CERT/CC) at Carnegie-Mellon University** at http://www.cert.org. CERT/CC is a nonprofit organization established to help detect and prevent computer security breaches. CERT/CC policy is to keep information specific to your site confidential, unless they receive your permission to release the information. This is an excellent resource for computer systems security issues and guidance.

There are also a number of security alert services. An example of such is: http://www.sans.org/nwcnews

Employee Termination Computer Checklist

It is proposed that we have a "Computer Termination Checklist" for all employees, students, volunteers, etc. who have been granted access to computers or automated systems and who have left or graduated or been promoted. When employees leave the SDOC they are often required to turn in keys, credit cards, sign termination forms and complete other requirements of the human resources termination checklist. When employees are terminated, the process should also include completing a questionnaire similar to the following:

I. Do you have a laptop, desktop or other computer equipment at your work sites, at alternate work sites, at your home? (It is surprising how many employees leave with a SDOC computer or with files containing secure data.)

II. Do you have any disks with important, proprietary, confidential or sensitive information on them?

III. Do you currently have access to SDOC computers? If so, which ones?

IV. Has your user identification code and password been canceled?

V. Did you delete or substantially alter any computer data, files or programs upon your termination?

VI. Is there any reason that the SDOC cannot access, or will have difficulty accessing, computer information previously controlled by you?

VII. Lastly, require a terminated employee to sign a statement that they not try to gain access to any of the SDOC's computer systems or provide information to help others gain access to SDOC computer systems.