
# *Technology and Computer Use Guidelines*

## Table of Contents

**Note:** These materials are a combination of policies, guidelines, and explanations from a variety of sources; including information from LCSB staff. The sources are sufficiently widespread and have occurred over such a large time, it is not possible to provide proper credit to all the sources and authors whose work is included within this document. All those contributing to this document, and those who contribute to the continued improvement of these guidelines is recognized and appreciated. It is intended that this document help serve to educate those of us responsible for the education of LCSB students, whether directly, as teachers; or indirectly, as staff, managers, and administrators.

# Purpose

The purpose of the Technology and Computer Use guidelines is to help protect the Leon County Schools (LCS) and employees of the LCS from liability and business interruptions due to inappropriate use of Leon County School Board (LCSB) computers and breaches of computer security.

This guideline documents the computer users' responsibility to safeguard computer equipment and information from accidental or deliberate unauthorized access, tampering, phishing, distribution, or destruction. It sets forth what is, and is not, appropriate use of LCSB computers. Users may be disciplined for noncompliance with LCSB policy and procedures. This guideline does not purport to address every computer operating and security issue. It is the user's responsibility to use sound judgment. Should you identify an issue or situation that you are not certain how to deal with, contact your supervisor or Technology & Information Services (T&IS) department.

The Technology and Computer Use guidelines is subordinate to any collective bargaining agreement, employment contract, or other employment agreements. LCSB may add to, or change, the policies/procedures at any time. It is expected that any user, technology contact or specialist, or staff responsible for computer implementations or support be familiar with this guideline and District policy and procedures. Please read this material.

Any questions or suggestions for further improvements to our policies/procedures may be forwarded to Leon County Schools' Technology & Information Services.

# Introduction

Today, many people have access to computers. With the continuing increase in the power of computers, and the number of employees using computers, the time spent on computers can only increase. Because so much important work is stored on computers, and computers are used for transmission of student and business records, it is important that guidance on proper use of computers is provided.

The impact of the computer on our operations has been significant, and at breakneck speed. The technology accessible today could not have been speculated just five or ten years ago. Who knows what we will have available to us in a few more years. Keeping technology current is key 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. We do not have to look very far to find numerous examples of agencies that have incurred substantial losses due, in part, to the computer.

## The first, best, and most important line of defense starts with user education!

It is unquestioned that a well-trained work force properly versed 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, networks, or the internet. For this reason, we have created Technology and Computer Use guidelines. Please understand it is not our intention to encumber your use of the computer, but rather our fiduciary responsibility to protect the resources of LCS. We believe these procedures accomplish that with little to no hardship to you.

# Technology and Computer Use Guidelines

## Computer Users

Users are responsible for the appropriate use of LCSB 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 company computers, and 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 in accordance with policy guidelines, and 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 Leon County Schools this means access without appropriate specific authorization is prohibited.

In addition, any form of tampering, including phishing, and hacking, to gain access to computers is a violation of LCS policy, and carries serious consequences. Employees are required log off of their computer at the end of the day or when not in use for an extended periods of time. This will help prevent computer security breaches. In addition, computer users must take other reasonable precautions to prevent unauthorized access of company computers such as a password protected screen saver.

### Computer Sabotage

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

## Password Selection and Protection

Select difficult passwords. Change them regularly, and protect them from phishing attacks. A lot of damage can be done if someone gets your password. Users will be held accountable for password selection and protection.

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, or any other communication line.

Poor password selection and safekeeping is not comforting to LCS staff investigating a computer security breach, nor is it an acceptable excuse if a hacker damages LCSB computer systems using your password.

## 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 LCSB policy.

## 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. For example, if you live on Elm Street, do not select "elm" as a password. Select the nearest crossroad and always finish, or start, with a number (maybe your youngest child's age).

The following are our current password requirements:

- Minimum length of 8 characters with three (3) out of four (4) of the following conditions met:
  - Must contain an uppercase letter
  - Must contain a lowercase letter
  - Must contain a special character
  - Must contain a number
- Your password should be change on a regular basis and at least once every 60 days where there is a significant risk relating to personally identifiable confidential information being accessed.

- Your password should not include your login name, your name, your spouse's or partner's name, children's or pet's name, or any other names commonly known to others
- Your password should not be a word pertaining to the LCSB, your work, or an activity that you participate in or follow that is commonly known
- Your password should not include anything derogatory or offensive
- New passwords should be unique in terms of those used recently

If you have a question about password selection or safekeeping, please contact your Technology Contact or T&IS.

**Password Access**

Effective passwords are an excellent tool to defend against unauthorized access of LCSB computers. However, a password is only effective when used properly.

Do not leave your computer logged on and unattended for an extended period of time. Do not log on to your system if someone can see you keying in your password (there is no need to create the temptation). Log off your computer when you leave at night. If you use a remote access program, and you need to leave your computer on, be sure that it is in a locked room. Furthermore, use a password protected screen saver to secure the computer from unauthorized access.

**Snooping**

*Snooping* -- an affectionate term common in the English language. Defined in Webster's Dictionary as "to pry about in a sneaking way."

Snooping into LCSB computer systems is a serious violation of LCSB policy. If you have no business being there, don't go there. If you accidentally identify a new way to access information, report it to your Technology Contact or supervisor. Watching other users enter information, and looking at computer files 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 LCSB policy and are likely violations of state and federal statutes. If you observe someone snooping, report it to your Technology Contact of supervisor.

**Hackers**

Hackers work 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 or emailing unsuspecting employees representing themselves

as a new employee, executive of the organization, or another trusted individual. This is called phishing. Through a variety of probing questions, they attempt to obtain the information necessary to breach the security of our systems.

Never give any information about computer systems out over the telephone, or in any other way. If someone requests such information, get their name and phone number, and tell them you will get right back to them.

Report security incidents immediately to your school site or department management, and to the district's Technology & Information Services Help Desk (487-7524; helpdesk@leonschools.net). Without your help, LCS has little chance of protecting the LCSB'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 LCSB computers is prohibited, and will be reported to the local authorities. Hacker crimes result in millions of dollars of downtime, lost data, and other problems. If you are caught hacking, it is a serious offense. If you identify vulnerability in the LCSB's computer security system, report it to management.

**Phishing**

Phishing is the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers. K-12 districts are seeing a significant increase in the number of phishing attacks. Because of this, annual security awareness training is conducted and periodic emails to staff are circulated to remind them of the need to be very careful when opening attachments or clicking links even if the email appears to be from another LCS Employee. To aid in the identification of email from outside LCS you will see "EXTERNAL" in the header of the email to help you upfront identify emails that do not originate from LCS. If you suspect an email you received might be a phishing email, please forward it to phish@leonschools.net so that TIS staff can evaluate the email. If you suspect you accidently provided your credentials in a phishing email, reset your password immediately and contact your Techcon or TIS so that we may take the steps necessary to protect you and other district resources. To aid in training users on how to recognize phishing emails we employ managed phishing software regularly (at least once a year) to test/track district staff responses to phishing emails.

**Multi-Factor Authentication (MFA)**

Using two or more forms of identification to authenticate a user. The common single-factor authentication employs one password. For more security, multi-factor authentication adds at least one more form such as a text message with a

one-time number, a physical token or some form of biometrics. LCS uses MFA to protect district resources.

### Viruses and other malicious software

It is critical that users make certain that data and software installed on LCSB computers are free of viruses. Data and software that have been exposed to any computer, other than LCSB computers, must be scanned before installation. This includes e-mail with attachments (a virus can quickly contaminate your computer simply by opening an e-mail attachment), 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 site Technology Contact or T&IS. Use of viruses or other malicious software is prohibited.

If you identify a virus or other malicious software, do not try to fix the problem. Immediately turn your computer off, make notes as to what you observed, and contact the site Technology Contact and/or T&IS Help Desk (487-7524; helpdesk@leonschoolsnet).

The principal concern is stopping the contamination before additional damage is done. These programs are most successful when ignored. They are designed to easily hop from application to application, contaminate a files, and access another computer. They easily travel down phone, networks, 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. Turning off your computer does this best.

### Who You Can Contact if a Security Breach Occurs

**Any security breach relating to passwords or hacking of electronic data files or systems must be reported immediately (or as soon as emergencies permit) to the Technology & Information Services Help Desk (487-7524).** It is increasingly the case, particularly in the electronic medium, that “hacks” or “breaches” are widespread; that logs or records are more complete/detailed as these data are more current; and that appropriate legal and procedural steps be taken as consistently as possible. Typically, our effectiveness in minimizing damages due to a security breach and our ability to trace security problems is greatly improved where appropriate communications have occurred quickly.

## 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. Using confidential information for anything other than its intended use is prohibited, without prior management approval. The most common confidential data used in the district is student data which is protected by the Family Educational Rights and Privacy Act (FERPA). In addition, any health related data is protected by Health Insurance Portability and Accountability Act (HIPAA).

**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 with confidential files logged on to your system
- Storing confidential data on portable media that is not encrypted.

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

**Electronic Confidential Information Security Awareness**


While the underlying principals and applicable policies/procedures are the same, treatment of electronic versions of confidential, personally identifiable information is sometimes not afforded the same consideration or respect that is warranted. For example, in the old days it would be unheard of that a teacher would leave their grade book open on the desktop, with entries in pencil, with a pencil readily available – and then leave the room. However, it is not that rare that a teacher "signs on" to a grade book or to an AIP, or to an on-line test or grades screen; and then leaves their desk, allowing it to be seen (if not changed…) by others without legitimate educational interest. Both these situations are illegal, inconsistent with official policy and procedures, and the individual, their supervisor, the school, and the school district are liable and prosecutable.

It is the intent of this guide is to create awareness of the importance of our being mindful of these requirements, and prudent and reasonable steps to ensure appropriate security as relates to the collection, access, maintenance, distribution and destruction of confidential information – whether student or adult. This is the responsibility of everyone: teachers, staff, and administrators.

**Key Considerations**:

- Confidential information (student or staff) must be kept secure; from original collection through updates, routine access, maintenance, distribution (whether hard copy or electronically posted via browsers) and destruction.
- Only those with legitimate educational interest can access confidential information. Those persons should be authorized in writing, provided passwords, and understand the importance of maintaining security.
- When persons are provided access to such information, prior written authorization must be on file, renewed annually or as job duties change or as transfers or graduation dictates. This also pertains to those working with data files, archived data, password files or records, or any technology or network systems technical support tasks.
- Student access to data files, systems, passwords, etc. that could result in security breaches must be carefully monitored and restricted to only what is essential. Anyone working with confidential data or security systems must have prior written authorization.
- Authorizations, passwords, system access codes, and passwords must be updated/terminated/changed as transfers, job changes, graduation/program changes occur.
- These considerations apply to remote access, and to stored files; again, regardless of whether these are electronic or hardcopy.
- Access to confidential records, files, data must be logged such that questionable instances can be evaluated and access or changes to such data can be reasonably monitored. Physical or electronic location of such information must be such as to reasonably restrict and control access for appropriate purposes and by authorized individuals.
- Any significant security breach relating to passwords or electronic data files or systems must be reported immediately (or as soon as emergencies permit) to the Technology & Information Services Help Desk (487-7524) It is increasingly the case, particularly in the electronic medium, that “hacks” or “breaches” are widespread; that logs or records are more complete/detailed as these data are more current; and that appropriate legal and procedural steps be taken as consistently as possible. Typically, our effectiveness in minimizing damages due to a security breach and our ability to trace security problems is greatly improved where appropriate communications have occurred quickly.
- There is much more extensive information on policies/rules/statutes. Further explanations, forms, and guidelines are posted on the district’s web site

(www.leonschools.net).

## Physical Security

### Locks

Physical security is key to protecting your computer and computer information from loss and damage. Store memory devices (examples: USB memory keys, external hard drives, etc.) and other sensitive information in a locked drawer. Log 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. Your investment of time will provide an excellent return, and help prevent temptation by others.

### Mobile Devices

There are many sensible, cost-effective measures that can help reduce the risk of loss or damage of mobile devices. The following are things to be aware of before taking mobile devices from LCSB property:

- Mobile devices must be signed from your site with a Temporary Removal of Property form. This can be obtained on our LCS Forms site (http://leonschools.schoolwires.net/domain/108)
- Report lost or stolen computers immediately to your site Technology Contact.
- Be sure to backup your important files on a regular basis
- **You are prohibited from storing confidential information on mobile devices (examples: laptops/tablets) unless that device is fully disk encrypted. You will ultimately be held responsible for any confidential information, so protect it appropriately.**
- Use reasonable precautions to safeguard the mobile device against accidental damage (don't work on your laptop in the pool)
- When traveling, mobile devices must be in sight at all times or physically secure
- Always store mobile devices in a concealing carrying case
- Verify your home owners insurance will cover the loss of the mobile device due to theft or fire. You can be held responsible for the replacement of the device in these situations.

### 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 approval.
- Adhering to all computer policies and practices of the LCSB for on-site users.

## Administrative Matters

### Storing of Confidential Data (FERPA, HIPPA, etc.)/Backups/Re-imaging

**All confidential data must be stored in District approved secure storage. These are: LCS network drives or Microsoft OneDrive.** Storing confidential data anywhere other than the approved storage locations mentioned above must be encrypted. Confidential data being transmitted must be encrypted (for example: sending a confidential file via email).

Storing information on the local hard drive of your computer is strongly discouraged because of the potential for hard drive failure. In addition, if your system experiences a software problem that is not easily resolved it is very likely that your system will be re-imaged. If this occurs, you will lose any data stored on the local disk. Storage of confidential data on local hard drives (examples: desktops, laptops, tablets) is prohibited. Use the approved storage locations for confidential data as indicated above.

Approved storage locations have security systems in place to protect the data and are backed up on a regular basis.

### Copyright Infringement

The LCSB does not own computer software, but rather licenses the right to use software. Accordingly, LCSB licensed software may only be reproduced by authorized LCSB 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. There is no “but copying it was so easy” defense to copyright infringement. Copyright infringement is serious business, and the LCSB strictly prohibits any such activity. If you have questions about copyright infringement, discuss it with your site administrators.

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. As such, it is important that you check with your site Technology Contact before downloading/installing shareware or freeware.

## Harassment, Threats and Discrimination

It is LCSB policy, and the law, that employees are able to work free of unlawful harassment, threats, and discrimination. Unlawful harassment is physical or verbal/written actions 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. Currently, there are many cases in the courts addressing just such issues, the ramifications of which are significant. The computer is possibly the easiest tool for obtaining, storing, sharing, and disseminating to large audiences such material and viewpoints. Stay away from such activity; it is a serious violation of LCSB policy. It is inappropriate to use LCSB 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 LCSB. LCSB computers are not vehicles to express free speech. Do this on your own time, away from the LCSB, 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 LCSB 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-work related 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 LCSB.

## Unauthorized Changes to LCSB Computers

Installing software and making changes to computer hardware, software, system configuration, and the like should be coordinated through your site Technology Contact. 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.

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 LCSB computers

The list of potential problems goes on and on. Accordingly, talk to your site Technology Contact before making any changes to LCSB computers.

**Operating System and Software Systems Updates**

The district uses automated tools to insure operating system and software systems are running on supported versions of operating systems/software. It is important that these devices are regularly connected to the network so that all systems are running the correct versions. This is especially important for mobile devices that may be used at home. Mobile devices should be regularly be brought back into the office and connected to the LCS network to receive critical patches and updates. This is important for the safe and smooth operation of your computer systems. The practice of updating operating systems and software is a never-ending process with our goal to implement zero-day updates ASAP and all critical updates within 7 days. If you suspect, for some reason, that your device or software is not running the latest versions please contact your Techcon or TIS for the latest updates.

**Remote Access to District Resources**

LCS allows remote access to our network via Virtual Private Network (VPN) access. A request for remote access is not automatically provided. Each request will be evaluated based upon justification for such access and must be approved by TIS before authorized. If you wish to remotely access our resources, you must complete the VPN access approval form. This can be requested from our security department. VPN also requires Multi-Factor Authentication to gain access to LCS resources.

**Purchases of Computer Software and Equipment**

Purchases of computer software and equipment must be coordinated through your site Technology Contact or T&IS. Technology Contacts and T&IS are familiar with technology standards and other compatibility requirements

necessary for computer software and hardware to work correctly in the LCSB technology environment.

## Disposal of LCSB Data

Purge files that no longer have a practical use or a required retention period because they take up precious storage space. A word of caution: permanently removing a file 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 time consuming for your site Technology Contact or T&IS to recover a file from backup tapes.

## File Recovery

Computer files and e-mail are rarely erased from the system simply by hitting the delete key. Rather, they are stored in a random place on the computer. These files can be easily recovered by running a file recovery program. To actually erase a deleted file from existence, you must run a program to erase deleted files. Keep in mind that if the files are backed-up before you run the program, you again have an electronic record. Files stored on the network are much more difficult to erase. This is because the network is backed up automatically via a regular schedule, and only your Technology Contact or T&IS have access to run programs that will permanently erase a file from the server. The bottom line is, your deleted file is most likely permanently stored on back-up. All emails are permanently captured in the District email archiver.

## Personal Use of District Computers

Incidental and occasional personal use of LCSB computers is permitted for reasonable activities that do not need substantial computer disk space, interfere with work requirements, or other computer equipment. As a general rule, if you would be uncomfortable asking for permission, it is probably not an appropriate use of LCSB computers. Prohibited activities include, but are not limited to, computer games, personal software and hardware, writing your autobiography, and running a personal business on the side. Using LCSB computers to store or transmit inappropriate jokes, junk mail, chain letters, or to solicit for commercial, religious, charitable (unless approved by your site or LCSB), or political causes is prohibited. If you are uncertain about a specific activity, ask your supervisor. Personal files, information, and use of LCSB computers will be treated no differently by the LCSB than business use, with regard to employee privacy.

Many software games and other software are illegally copied, and often contain viruses. Such programs represent a potential liability to you and the LCSB. Proof of ownership and site administrative approval for use is required for all software not specifically purchased/approved by LCSB.

## Use of Personally Owned Devices on the District Network

The District provides a device to each student for use in the classroom and at home (if allowed by the school to be taken home). The District provided system is the only authorized system for the classroom. The District provides both a guest network and business network. The business network is a secure network for the conduct of official School Board business. Access to the business network requires prior approval and authorization by the District. The guest network is CIPA-compliant non-secured network provided for use by students, parents, and other visitors while on school property.

## Proprietary Information

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

## Reporting Policy Violations

Employees are required to report violations, or suspected violations, of computer policy. Activities that should immediately be reported to the site Technology Contact or T&IS include, but are not limited to:

- Attempts to circumvent established computer security systems
- Use, or suspected use, of malicious software
- 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 LCSB, or an employee of the LCSB, in any way

Computer policy violations will be investigated. Noncompliance with the LCSB's employee computer policy may result in discipline up to, and including, termination. Employees that report violations, or suspected violations of LCSB policy 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 a computer security vulnerability, you are required to report it immediately.** Call the Technology & Information Services Help Desk (487-7524) or Technology & Information Services main office (487-7530). 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 LCSB property. Deleting, altering, or sharing confidential, proprietary, or any other information upon termination requires authorization. The computer you have been entrusted with must be returned with your password, identification code, and any other appropriate information necessary for the LCSB to continue using the computer, and information, uninterrupted. See the "Employer Supervisor Exit Checklist" on the forms website (http://leonschools.schoolwires.net/domain/108) for an employee leaving the employment of LCS.

The following activity is prohibited upon termination, and individuals involved in such activities may be prosecuted to the fullest extent of the law:

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

## Employee position changes—Administrator/Supervisor responsibilities

The following are the responsibilities for administrators/supervisors when and an employee changes positions or is no longer employed by the District. These responsibilities are based upon a concern for security and accounting for data and equipment – in meeting both the school district's and your own personal interests. The administrator or supervisor, in addition to the person in the position, is responsible to seeing that these responsibilities are addressed. The employee supervisor checklist (available via the district forms website) should be used to guide this process, and with appropriate sign-off to document the completion.

1. **Documents, Email, or Files**: Make copies of or assure ready access to particular documents or files that your successor, interim assignee, or supervisor should have: official correspondence, reports, data, works in progress….

a. Your files (documents, data, email, etc.) saved on the network file server will remain accessible to your supervisor. Your supervisor (or anyone authorized by the supervisor) will be authorized to access these files and everything contained within.

b. Forward any still-in-progress or action items (e-mails, drafts, etc.) still pending to whoever should continue to be involved with those items.

c. As of the day after your leaving this position your e-mails will be forwarded to whoever you or your supervisor designate. One or two days prior to your leaving the position, please use the Tools/**Out of Office Assistant** so that all incoming mail sent to you will notice senders with a message similar to the following: "*your name* is no longer in this position; all e-mail is being forwarded to _____; please contact this office for issues or questions relating to the *title of position vacated*" General network access is disabled, i.e. access to files, network-resources and applications, upon notification of termination. Only with the position supervisor's approval and request, accounts may be modified to allow email access for a period of 30 days after position termination.

d. If you have hard copy paper letters, reports, etc. that you prefer to have in electronic copy form, it is recommended that you scan these to a file as PDF documents.

2. **School District Equipment**:

a. Leave computers, mobile devices, and phone devices with the office or with the person issuing that item;

b. Copy and keep, and then delete any confidential or official correspondence or information from all such devices. All official correspondence should be kept on file – electronically, such documents and files should be kept on network resources. Let your tech specialist know who should be authorized to access these files as of a specified date. If assistance is needed, contact the Help Desk.

c. Your computer will be re-imaged following the vacating of your position. All standard functions (e-mail, Internet access, standard office tools…) will be refreshed, but all stored files and non-standard programs on the computer – not those on the network server - will be erased. All fields and all programs on the computer will be erased.

d. If the equipment is to be transferred or salvaged. The following procedures apply to remove possible sensitive data:

- Prior to transferring a computer:
    - From one person to another within a site, re-image the system.
    - From one site to another, re-image the system (responsibility of the site that is doing the transferring)
- Prior to salvaging a device that contains data storage (examples: computers, printers): All data must be removed from device before salvage (example: hard drives). You have three options for the removal of all data from a computer system before salvage:

- Degauss: T&IS maintains a degausser (a device that removes all data through a magnetic process) that will render the drive unusable/unreadable. You can bring your hard drives to T&IS and we will degauss them for you. This is the preferred method.
- Destroy: You can destroy the hard drive by drilling through the hard drive platter and electronics.
- DBAN: For hard drives that are still working in a system, you can use software called DBAN that writes a series of zeros and ones multiple times to remove all data. This is a time consuming process and is the reason we suggest degaussing as another option.
- Solid State Drives: Special utility software must be used to erase SSD. Contact T&IS for available options.

3. **Automated Systems Access & Authorizations:** Your authorizations to the school district's enterprise information systems or networked equipment (student, finance, or staff) will be scheduled for removal as of this position being vacated. Please let district's Information Security Office (T&IS; 487-7530) know if any exceptions should apply. You or your supervisor should notify T&IS Help Desk of the date you will be leaving your position. While personnel listings are also shared, this may not be as immediate as your sending an e-mail to T&IS Help Desk (helpdesk@leonschools.net).

RESPONSIBLE USE REQUIREMENTS: System access responsibilities, carry responsibilities for users; school and district site/department supervisors; technical support staff (at both school and district levels) and automated system managers; and program/district administrators.

- o Users: All users are expected to be responsible for their own access and actions, consistent with School Board access use policies and consistent with the (Employee/Volunteer Internet Use/Access AUP Permission) form and the Student Internet Use/Access Permission form. The Internet Access/Use form must be signed before a user is provided a user name/ID and network or system password. If application access is granted completion of the Security User-ID Agreement is required.
- o Supervisors (cost center managers and those responsible for hiring/evaluation): All supervisors are expected to be responsible for appropriately authorizing and de-authorizing employees and workers under their supervision. Supervisors must request application access for those who require access to the business system (Skyward Access Request Form) or Foucs (Focus Access Request Form District-Wide Staff (Non School)) applications by completing the required forms. Timely assignment and de-authorizations of network and system access, and – in particular - the specific authorizations within automated systems (e.g. read

access to payroll or student emergency contact information) are the responsibility of the supervisor/administrator. When position changes (terminations or transfers) are made, the **Employee/Supervisor Exit Checklist** and the Personnel Procedures/Manual must be routinely followed as intended. Most critical, is that supervisors must update access rights as positions are changed, and notify their site tech specialists or district program/security staff in timely order.

- o Program and District Administrators: Program and district administrators are responsible for oversight of users and programs in their respective areas; to provide for user awareness and training, and to monitor users and managers to see that security policies/procedures are followed. Specifically, to confirm that authorizations and de-authorizations are handled in a timely and appropriate manner.

    - o Technical Support Staff:
        - At the school or department level: Tech specialists (or those assigned technical specialist duties) are expected to assign and terminate network and systems access as new employees are placed or terminated/transferred. This must be done in timely order as soon as hires or appointments are made or changed. It is the site or cost center manager's responsibility to see that position changes are communicated to the respective tech specialists, and that there are adequate resources provided for system security changes.
        - At the district level Tech specialists will routinely:
            - Respond to requests for position access or authorization changes (typically within 24 hours);
            - Confirm position terminations relating to network and enterprise systems authorizations based upon Personnel Action Form (PAF) terminations of record (typically weekly);
            - Periodically disable access of users who have extended periods of system non-use (at least annually, following the end of the regular school year);
            - Annually prompt administrators to review and update network and systems access/authorizations.

- o For further information contact the program area administrator (payroll, budget, student enrollment, etc.) or the Technology and Information Systems department (T&IS).

## Privacy/Data Security

## Monitoring Computer Communications and Systems

Many people think data stored on computers, transmission of data over communications lines, and e-mail are private, and in most cases they are. However, the LCSB 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 LCSB computers are clear of viruses, and used in accordance with LCSB policy, may be performed. The LCSB will investigate complaints about inappropriate images on computers, inappropriate e-mail, or other inappropriate conduct. The LCSB 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 LCSB property, and should be used principally for business purposes.

## Family Educational Rights and Privacy Act (FERPA)

FERPA is a Federal law that protects the privacy of student education records. We are all responsible for protecting that information as we use automated systems, create files containing student information, and sharing that information with others. Before sharing student information, make sure you check with administrators at your site to make sure you aren't violating FERPA rules.

## Children's Internet Protection Act (CIPA)

The Children's Internet Protection Act (CIPA) was enacted by Congress in 2000 to address concerns about children's access to obscene or harmful content over the Internet. CIPA imposes certain requirements on schools or libraries that receive discounts for Internet access or internal connections through the E-rate program – a program that makes certain communications services and products more affordable for eligible schools and libraries.

Our responsibility under CIPA is:

- Control access by minors to inappropriate matter on the Internet;
- To ensure the safety and security of minors when using electronic mail, chat rooms, and other forms of direct communications;
- To prevent unauthorized access, including so-called "Hacking," and other unlawful activities by minors online;
- To prevent unauthorized disclosure, use, and dissemination of personf information regarding minors; and
- Implement measures restrict minor' access to materials harmful to them.

## Web Filter

To ensure compliance with CIPA, we use a CIPA compliant web filter to protect our Leon County School Board users.

### Proxies/Personal VPNs

To minimize the ability for someone to bypass our protection put in place to make the Internet a safer place, we do not allow the use of proxies or personal VPNs on our school district network.

### Data Privacy/Data Security

Privacy of staff and student information is paramount. For rostering of staff/student data with third party vendors, we require a Data Sharing and Privacy Agreement to be signed by the vendor to ensure the protection of data given to vendors.

### Lawsuits and Subpoenas

LCSB computers, like any other LCSB property, are subject to subpoenas. This means that prosecutors and plaintiffs' attorneys may access LCSB computers, and look at information to gather evidence in a complaint. It is important that users conduct their work to the highest ethical standard with the knowledge that computer information (even deleted files) can be used 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 LCSB computer systems. Accordingly, only LCSB employees are allowed access to the LCSB's computer systems, without written authorization from your site administrator. Your site administrator 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

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. 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 site administrative authorization is prohibited. Furthermore, the following non-business related activities are prohibited without site administrative authorization:

- Accessing the Internet without an approved firewall
- 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 LCSB

Individuals that have received site administrative approval to transmit information on the Internet should understand that such transmissions are identifiable and attributable to the LCSB. Disclaimers such as "***The opinions expressed do not necessarily represent those of the LCSB,***" while a good idea, do not necessarily relieve the LCSB 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 LCSB 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 LCSB policy, or is contrary to the LCSB'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 LCSB, and the law, can and will hold you responsible for offensive, discriminatory, and defamatory statements, or any other illegal activity.

## E-mail

### Electronic Communications

E-mail is a wonderful tool. Used correctly, it can provide significant efficiencies, and improve the quality of the way we do business. It makes dissemination of information easy and cost-effective.

The same standards of decorum, respect, and professionalism that guide us in our face-to-face interactions apply to the use of e-mail.

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

- Accessing, or trying to access, another user's e-mail account
- Obtaining, or distributing, another user's e-mail account
- Using e-mail to harass, discriminate, or make defamatory comments
- Using e-mail to make off-color jokes, or send inappropriate e-mail to third parties
- Transmitting LCSB records within, or outside, the LCSB without authorization
- Transmitting junk mail, chain letters, or soliciting for commercial, religious, charitable, or political causes

Employees are required to report inappropriate use of e-mail.

### Dangers and Pitfalls of E-mail

Appropriate e-mail 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 e-mail. However, e-mail does not disappear into thin air. It can be widely, easily, and quickly disseminated. E-mail can be edited, forwarded, distributed, and filed for later use, possibly at the most inopportune time. For professionals with electronic recovery skills, e-mail is a gold mine. If you would not put it in a memorandum on LCSB letterhead, do not say it with e-mail!

### Forwarding Information

Automated forwarding of E-mail is prohibited (AP 7530.03 – District Approved Applications for District Business). E-mail 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 e-mail (particularly e-mail 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?
- Does the attachment contain confidential information? If yes, be sure to encrypt it.

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 only result in misunderstanding, hurt feelings, and added work.

**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 LCSB policy and will be prosecuted to the full extent of the law.

## Intranet

The LCSB Intranet, like e-mail, is a wonderful tool. It 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 LCSB personnel are allowed access to the Intranet, without written authorization from

management. All LCSB policies apply to use of the Intranet. The following activities are prohibited, without site administrative 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 LCSB in obtaining access to the Intranet
- Making any changes to the Intranet hardware or software

# Glossary of Terms

## Computer Information
Data, software, files, and any other information stored on LCSB 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.

## 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.

## LCSB

Leon County School Board or Leon 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.