PS-131

Employee Technology Handbook

Appropriate and Effective Use of Technology Resources

Includes Important Password Security Information and User Responsibilities

Sumter County Schools
2019 - 2020

HIGHLIGHTS AND CHANGES

- **SECURITY – Check daily to make sure Kaspersky is running.**
- **GEO Blocking on firewall will prevent accessing receiving data from other countries. Data security is everyone's business**
- **Phish Alert Button in Outlook and Office 365 portal**
- **Data Loss Prevent (DLP) will send emails indicating your e-mail had sensitive data in it. "Your e-mail message conflicts with a policy in your organization."**
- **Store the most sensitive data on local protected shared folders.**
- **All computers\laptops must be signed in on our network at least once a week or will be disabled.**
- **Coming soon to a browser near you! Clever 2.0**
- **Windows Update – Are automated if the computer is allowed to download, install and reboot correctly. The desktop Windows Update button is there if you would like to confirm your computer is up to date.**
- **All wireless access points have been upgraded to the new model.**
- **New work order / laptop sign out program "One to One Plus" for the 19-20 school year.**

INTRODUCTION

Our school district recognizes the potential of technology to support innovative means of instructing students and providing tools for using technology.

Instructional technologies and telecommunication services will be used to support, enhance, and optimize educational endeavors, as identified through the Florida Standards and other curricular expectations, in a coordinated fashion spanning all grade levels, disciplines, and programs where appropriate.

Technology advancements have brought forth new possibilities, but at the same time has opened new situations that require us to better understand the legal aspects and other conditions affecting how we instruct students and manage the school district. Schoolteachers, through their professional duties, have access to information that is confidential. Several federal and state laws, particularly the *Family Education Rights & Privacy Act (FERPA)*, requires stringent protection of information about our students. Years ago the risks of a breach was somewhat limited, today, through our technological tools, a simple error or careless act could cause broad access to confidential information. Connectivity and technology provide access to information and to learning opportunities, but also requires careful guidance and classroom management to protect, guide, and use methods to keep activities focused and effective.

Additionally, electronic files often contain information that is covered under Florida's broad open records laws as well as legal discovery requirements upon subpoena.

In order to meet the goal of educating our students successfully and providing services efficiently, this guide should provide assistance and support for efficient and instructionally sound use of technology services in the Sumter District Schools. We encourage a thorough review of this guide and keep it as a reference. If you have questions, contact information is provided throughout this document.

TECHNOLOGY

Staff E-Mail is provided for the specific purpose of supporting the educational missions of the Sumter District Schools and is archived. Email may be released when a proper information request is received.

- LIMITED personal use of email is permitted as long as it does not interfere with instructional goals and operations of the district. **This account is not a replacement for a personal email account.**
- It needs to be understood that under Florida's relatively open public information laws, no email messages are to be considered private. While personal e-mails are not necessarily covered by the open records laws, they may be released in a broader information request. **The district should not be expected to redact any personal emails or individual personal information that may have been sent via the district email system while used for personal purposes.**

Internet Access is also provided for the specific purpose of supporting the educational missions of the Sumter District Schools

- All access is governed by school board policy.
- Student access, with limited exceptions specified later in this document, requires a signed parental permission form.
- LIMITED personal use of Internet access is permitted as long as it does not interfere with the instructional goals and operations of the district and is compliant with the acceptable use policies. **Personal use during student contact times is not considered acceptable.**

Network and computer service access is protected by accounts requiring the user to login with their username and a password.

- **Users should NEVER provide their passwords to their accounts to anyone**.
- Logged in computers are to be locked (control-alternate-delete) whenever the user needs to leave the computer unattended.
- Accounts must be protected through complex passwords that are updated regularly.
- A common way unscrupulous hackers attempt to gain your account information is the use of fraudulent phishing emails. These are difficult to filter since often they use compromised

legitimate email accounts to send their attempts. **Never follow a link in an email that is requesting personal information including login credentials.**

The Student Information System (SIS) and Business Information System (BIS) in our District is Skyward and is managed by the Management Information Services Department. MIS handles operations related to Skyward Questions concerning Skyward Data can often be handled by the Data Entry Clerks or Secretary at your school site otherwise directed to MIS Support @ ext. 50240 or (**Jessica.Temple@sumter.k12.fl.us**).

Technology Problems: Most technology problems should be reported to the Help-desk. Often the help-desk will have an immediate solution for you or will be able to coordinate Level 1 or Level 2 Tech support to resolve all tech problems. To contact technology support, you can create a technology work order (found under Sumter Links in Favorites), email support@sumter.k12.fl.us or calling 352-793-2315 ext. 50250. Important information necessary to expedite service includes: 1) the computer (decal) number, 2) the user that was logged in when the problem occurred and 3) as clear description of the problem as possible, including the wording of any error messages.

I.T. Coordinator: David Trick
david.trick@sumter.k12.fl.us 352-793-2315 ext. 50296

Network Assistant: Tina Mansfield
tina.mansfield@sumter.k12.fl.us 352-793-2315 ext. 50222

Server Assistant: Nicole Stiefel
nicole.stiefel@sumter.k12.fl.us 352-793-2315 ext. 50264

SECURITY AWARENESS

The technology resources of the Sumter County Schools contain access to privileged information. This along with the importance of these resources for day-to-day business / educational activities, creates a situation where all users must be aware and use the resources in a secure fashion. Since teachers and staff accounts have access to sensitive data, we require a higher level of security than we require of student accounts.

Security Breaches: Data housed in the various information systems throughout the district often contain protected and/or sensitive data

that if destroyed, changed, or released may put individuals or the district at risk. It is imperative that you report to tech services ANY activity that shows a possible breach of security. Report suspicious technology use immediately to your principal/supervisor **AND** technical support (support@sumter.k12.fl.us) Phone: 793-2315 ext. 50250

Passwords Must Remain Secure

- **NEVER** share your password or allow anyone else to use your login information. Users are responsible for activities that occur under their login.
- Under **NO** circumstances should passwords be marked or labeled on or near a computer
- **NEVER** allow students to work from your computer while logged in under your account

Secure physical access to your computer

- Your computer screen should not be easily seen by others in the room since you are likely to have protected data, such as your grade book open
- You should lock your computer account whenever you are not physically able to protect your computer from access from others
- Your computer will lock automatically after 15 minutes of inactivity.

Protect Your Computer System and the Network

- Our systems are set to automatically download updates. It is important that all systems are kept updated. Please do not disrupt the installation.
- There is a distinct possibility you may receive a popup reporting that a virus has been detected. This is a sign the software is performing as it should. Currently the district uses *Kaspersky* Antivirus software on the computers. The antivirus software is running properly if the icon is found near your clock. It is common practice for web sites to post "fake" virus messages, often trying to sell their "security" products. If the warning appears in a web browser page, it is not from our system and could be a risk if downloaded.

- **All computer users** should verify that **Kaspersky is visible** in the **System tray** in the lower right hand corner daily. If the red K is not visible, a work order should be entered immediately as this is a security risk to our network.

- Use caution when downloading files and installing programs. If a download prompt appears when you are not expecting it, please cancel.
- We do not recommend the installation of "search bars". These search bars typically do little more than slow down your system and reduce screen area for Internet browsing. Often they are options when downloading software, including required applications such as Acrobat Reader or Java. Please uncheck before downloading.

- The user must be aware that copyrights must be respected and that any terms and conditions be followed for any downloaded software or content.
- Care must be taken to verify malicious software is not downloaded or installed within the network. The user accepts all responsibility for applications or software installed on the district's technological resources.
- Personal devices may only connect to the district's "internet only" wireless network. The wired and the "District Network" wireless network are only to be accessed by district owned devices.

Protecting Your Identity

- Do not reveal personal information inadvertently.
- Never use your district email account to sign up for non-work related mailing lists, contests, etc.
- Your work email is archived and web activity is logged. We recommend that personally sensitive issues not be the subject of emails or web searches at work.

Phishing

- There is a rising trend where SPAM emails are sent in attempt to trick the recipients to give personal data. Such attempts are called phishing. NEVER reply to any unsolicited request for personal information. Many phishing attempts are quite sophisticated and look very legitimate. The district DOES send emails letting users know their passwords are about to expire — BUT you are directed to use the network reset systems, not ask to click a link in the e-mail.
- Phish Alert V2 – A Phish alert button is now available in Outlook and Office 365 to report suspected Phishing e-mail to Support. If you suspect a Phishing e-mail please select the Phish Alert button and a new pane will open asking if you would like to report this email as a Phishing E-mail. Please select Phish Alert in the

pane and your e-mail will automatically be forwarded to Support with the relevant information.

Protecting Your Professional Reputation - Responsibilities and Liabilities

- Use proper spelling and grammar when writing emails, particularly within the district's email system.
- Never create an email in haste, anger or duress. Keep all communications to facts that you can substantiate. Digital evidence has become quite powerful in legal situations.
- Educators are held to a high standard of ethics. Keep in mind that your students and parents often have access to these websites and unprofessional behavior may have ramifications.
- Please keep a professional distance between yourself and your students. The modern world of social networking opens the door to more situations where the separation between your personal and professional life has become more ambiguous and as such, risky to a professional educator. Questions of impropriety are taken seriously by the district and the state Department of Professional Practices.

RISK FACTORS FOR SECURITY BREACH

It is imperative that all staff takes technology security as seriously as they do physical security, if not more so. While an unlocked door may be exploited by an individual that happens to be in the vicinity, a technical "unlocked door" can be exploited by individuals and syndicates not only locally, but also worldwide. The district operates sophisticated security "locks" that limit much of the risks but the possibility of a data breach is still possible.

Our greatest risks factors for a security breach include:

- **Social Engineering:** The greatest risk to the security of the network, users and the data available through it is to gain the confidence of individuals with access to the resources. This is done through various means, but the most prevalent technique we see are emails or websites warning the user that a problem exists and they need to complete a form that requests personal information which may include their username and password.

Sometimes they request personally identifiable information such as birth date or social security number, which adds substantial risk not only internally, but to the user themselves. Social engineering may also occur from other means of contact, including telephone calls.

- **Unauthorized Users:** While students and certain staff may have access to parts of the network, they are restricted from other areas. If a student or other person has access to another staff member's account, this could violate an individual's privacy or allow changes to data which is improper. For example, a student with access to their teacher's account may have the ability to change grades, attendance or other data. It is important to remember that with web based access to applications, an unauthorized user, with valid login credentials, could make changes from any location, day or night.

Malware / Viruses/ Trojan Horses and Other Malicious Software: Applications can be installed on your computer that can cause security issues. These can take several different forms such as:

- Keystroke logging - which records the keystrokes and transmits the information
- Email server - which allows the computer to send spam/phishing emails
- Redirection - where the computer redirects Internet requests to unintended/illegal websites
- Infection - where the computer is used to infect other computers
- Advertising/Unintended Websites - where your Browser opens additional windows with advertising or unexpected websites accessed. The impact may be annoyance to the user, slowing down the web experience, accessing unacceptable websites or placing the computer at risk of what is known as "drive by" infections where code is executed from the visited websites.
- Zombies - where the computer becomes a tool for the hacker to operate their applications or host their content
- Unknowingly installs software which slows your computer down and runs in the background, slowing the computer and the Internet experience. Quite often this is in the form of toolbars in your browser. Often, as a marketing ploy, an installer will have the installation of the extra software checked as a default add on.

Lost Computing or Storage Device: With technology becoming more mobile, the risk of data loss due to lost devices has grown substantially. Devices such as laptops are somewhat protected from unsophisticated

breaches due to the password protection, as long as the passwords are not available to the unauthorized person. **Under no circumstances should login information be recorded in a location accessible to someone who might steal or find a device, e.g. in the case or attached to the device.** All mobile devices with access to district services, including email, are to be protected with a password / lock code. Additionally, storage devices such as jump drives (USB drive), memory cards and external hard drives are another security risk. **No secured data should be placed on such devices.**

Connecting Unauthorized Devices to the Network: While the district understands and has policies that can support *Bring Your Own Devices* (BYOD), such devices are to be connected ONLY to the "Internet Only" wireless network. This network routes the traffic to our Internet Gateway, thus reducing the risk of unauthorized access to the primary network. The "Internet Only" wireless network will require authentication before gaining Internet access. Additionally, staff are requested to be vigilant and report any suspicious technological device found at the school site.

RECOGNIZING A POTENTIAL SECURITY BREACH

Indicators of a possible security breach may include:

- A lost device such as laptop, tablet, smart phone or storage device such as a jump drive (USB drive), memory card or external hard drive
- Noticing someone using another person's logon
- Noticing grade/data changes that you did not make within the grade book or other application.
- Your account has been disabled when you have not inadvertently entered the wrong password multiple times.
- Your password changed without your knowledge
- If you have provided your account information to another person, website, or through an email.
- If you begin seeing Kaspersky Antivirus alerts (Note: after legitimate Microsoft updates, changes may be noticed by the antivirus program. This is normal, but if concerned, please contact us.)
- You see antivirus alerts from unexpected "antivirus" programs
- If you begin receiving emails from unknown individuals accusing you of sending SPAM emails to them

- You notice your sent items folder in Outlook is suddenly empty or you stop receiving emails from others you know has sent you emails
- You notice missing or changed files within your user folder
- You notice students able to access inappropriate, personal web-based email or social networking websites while using district computers
- You notice students or unauthorized persons to be able to access staff only applications (i.e. Grade Book, Skyward, Email, Performance Matters, protected storage locations, etc.)
- Discovering an unknown device connected to a network connection anywhere within the site
- Observing any unauthorized person on or adjacent to school grounds using a computer wirelessly
- Observing an unauthorized individual opening the case of a computer
- Observing an unauthorized person attempting entrance to server rooms or telecommunication closets
- Noticing unexpected command windows (black windows on your computer screen) during operations (Note: command windows are normal during your computer login process).

REPORTING SECURITY BREACHES

It is imperative that network or data services personnel are informed immediately if there is a suspicion of a security breach.

1) Report suspicious technology use immediately to your principal **AND** technical support (support@sumter.k12.fl.us) and/or 7932315 ext. 50250)

2) If there is the possibility that your or another staff's password has been compromised, change it immediately and notify the Support desk!

3) Please take notes of the specifics of the possible infraction.

4) Report lost/stolen equipment immediately to the school & law enforcement.

5) If the breach involves student misbehavior, submit the appropriate disciplinary paperwork.

NETWORK ACCOUNTS

Various computer accounts are available to meet specific needs of teachers and students while assisting network services to meet the security and legal requirements related to modern technology access. **It is extremely important that passwords be safeguarded and kept private, preventing unauthorized access.**

Individual Staff Accounts: The accounts we create for staff members provide Internet access, E-Mail, a user folder to store documents, and the permissions and rights to access and use most services. Access to these accounts are not to be shared or used by others. **The named user is responsible for activities occurring under the account. New staff members should submit a form PS130 to have an account created.** Naming within this account should match the name on your Human Resource/Payroll record. When one changes their name, registered with Social Security, a new PS-130 form needs to be submitted to adjust the network account. Due to the number of applications populated using the Human Resources data, some applications will not work properly for the user if the names are different. Please note, contracted services accounts expire at the end of their contract or June 30th, whichever comes first. A new PS-130 is required to continue the account.

Individual Student Accounts: Student accounts provide access and use of many applications and programs. Internet access is available upon completing an Acceptable Use Agreement signed by the parent or guardian. The account provides a user folder for the student to store their documents. **In order for students to have Internet access, the student must receive parental/guardian approval.** Upon the return of the signed agreement, form PP-SR-059, the school technology contact will activate Internet access for the student's individual account. Please note, a school may choose to not require yearly forms, but is required to have the form on file. Student user folder contents may be deleted at the end of the school year.

Classroom Accounts: We are able to setup special classroom accounts to allow the teacher to provide student access to programs without requiring each student to login separately. By default, such accounts will only have student Internet access rights. It is required that such accounts only be used under the teacher's direct supervision, accessing sites specified by the teacher. **The responsibility to supervise the use of these accounts rests specifically with the teacher named in the account, so it is important to use only in**

locations under your direct supervisory control. These account will be required to be complex and passwords reset every 60 days. Submit your request on a PS-130.

Guest Staff Accounts: These accounts receive normal staff access to the Internet. These accounts do not have email or access to an individual user folder or a school's group-share. They are used for approved staff members to log in presenters or participants in training or unique work sessions. The named staff member is responsible for the password security and supervision of users of such accounts. Passwords are to be changed whenever it has been provided to a presenter or participant.

LOGGING IN

The Sumter District Network uses security features that requires users to log in with an appropriate account. In order to enter your login, you must press three keys together: Control (ctrl) Alternate (alt) and Delete (del).

You will then see the Acceptable Use Policy and must acknowledge your understanding prior to continuing. You will then see three fields to fill in:

1. USERNAME: Your username is your first initial and your EIN (Employee Identification Number).

2. PASSWORD: You will be given an initial password that you will have to change on your first login. All passwords must be a minimum of eight characters and include a mix of upper case, lower case, numbers and/or symbols (3 of these 4 complexities). The password field is case sensitive. When changing your password, you may not duplicate your previous 10 passwords.

PASSWORDS

As discussed earlier, it is very important to keep your password private. Password rules are enforced through technological means. You cannot change to a password that does not meet the complexity requirements required by policy. It is recommended that you create strong password that would be difficult to "crack" or particularly difficult for someone to understand by watching you login. Additionally, regular changes to passwords are required.

If you suspect that your password might have been seen or guessed, please change it immediately. To change a password, simply press Control (Ctrl) Alternate (Alt) and Delete, like you did to login and select "Change Password." You will have to type your old password in once, followed by typing your new password two times. This is done to make sure that there were no typographical errors.

Do not use the same password for all your personal and work accounts. Develop passwords that you "save" for your more sensitive uses, such as work and financial, and others for less secure situations such as a generic website requiring you to create an account. News reports have shown even large companies have had security breaches. By using the same passwords for multiple accounts you run a greater risk of compromised accounts that may lead to harm.

Please note, if technology support is requested to reset an account or create a new password, they will require evidence that the user is the requester. Email requests cannot be honored. All requests need to be in person (including with the school tech contact) or on the telephone. At minimum, the account name and the user's employee identification number will be required. Technical services reserves the right to request other information to verify the requester's identity.

COMPLEX PASSWORDS

Your network password must meet the following complexity rules:

- A minimum of eight (8) characters in length
- Be a combination of at least three of the following characters:
- Upper case letters
- Lower case letters
- Numbers
- Symbols
- The password cannot be a password that has been used in the past ten (10) times
- The password cannot be changed by the user more than once in a day.
- The password must be changed each 60 days.

When your password is nearing expiration, an email will be sent. Please note, it will NOT have a link to change your password, it will simply tell you to login in order to change it. Guidance, through the following sites, is available to assist in creating complex and secure passwords:

http://www.microsoft.com/security/online-privacy/passwordscreate.aspx

http://www.pcworld.com/businesscenter/article/187454/creating_secure_passwords_you_can_remember.html http://news.cnet.com/8301-19518_3-10310092-238.html

LOCKING YOUR COMPUTER

Through the day, you may have to leave your computer from time to time. Since your login provides access to your account as well as your files and any logged in applications, this could be a problem. Our computer system provides the ability to quickly lock your computer without having to log off. Once again, Control (Ctrl) Alternate (Alt) and Delete allows you to select the lock command. Also the shortcut of the Windows Key and the letter L will do the same.

To unlock the computer simply press Control (Ctrl) Alternate (Alt) and Delete and provide your password.
If a computer is unattended for a period of time, the device will lock automatically, but will provide a warning prior so you can abort the lock command. Unfortunately, streaming audio or video is not interpreted by the operating system as "activity." When streaming *Discovery* or other educationally appropriate material, one will need to watch for the warning so the presentation is not interrupted or use a "class" account, which due to its limited rights, does not automatically lock.

ELECTRONIC MAIL (E-MAIL)

One of the most used applications through the district network is Email. The service is provided to all staff members receiving a network account.

Your e-mail address is normally your first name<dot>last name followed by "@sumter.k12.fl.us." (i.e. Jane.Doe@sumter.k12.fl.us) As a convenience, the system supports "alias" addresses that also delivers to the same mailbox. Aliases can be provided to direct email from previous email account names in the case of name changes.

When using a Windows based computer within the district, the email client, **Microsoft Outlook** is used to manage your email access. We encourage you to review the other features of Outlook that may be helpful in helping you be productive. While your address book will be populated with the Sumter network addresses, by using the Contacts

portion of Outlook, you can add other frequently needed addresses. Additionally, the district "global address list" will have distribution lists that allow one to send to a group of people without typing all their addresses. Microsoft Outlook also provides an excellent calendar and scheduling system.

ACCESS WHEN NOT AT SCHOOL

The Sumter Schools also provides access to your email account from home or other locations with Internet access. To reach your account, you can go to **https://login.microsoft.com,** also known as Office 365 and log into your account. In the first box type your e-mail address. When you select the Tab key or click into the second box you will be redirected to a Sumter Federated Services login. Please provide your password to gain access to the Office 365 portal.
The password will be the same as you use to log in to computers at school.

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

If you have Microsoft Outlook installed on your home computer, it can be connected to your district email account and operate virtually the same as it does at work. When setting it up, you will need additional setup instructions. Please contact support for assistance. Additionally, we strongly suggest not using the CACHED mode unless you keep your mailbox clean and have a robust broadband connection.

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

- While limited personal use has been permitted, the school email account **is not a replacement for a personal email account**. Free or inexpensive web-based e-mail accounts are provided by several online companies including *Yahoo, Google,* and *Microsoft*, just to name a few.
- Florida has relatively open public information laws and no email messages, including personal e-mails, should be considered private and may possibly be released as public information. Also, the E-Mail system is the property of the School District of Sumter County. All E-Mail messages written using the system

are also the property of the District. Treat electronic communications the same as written hard copy.

- The District reserves the right to review all electronic correspondence that use District systems and facilities. In the case of a records request, there should be no expectation of privacy or the redacting of personal information from personal emails.
- In order to meet federal and state law, the Sumter School District archives electronic communications using its system.
- No personal technology use, including e-mail, should interfere with performing ones job function or interfere with others to perform theirs.
- One should not use their district account to register or list as their contact email for non-school related situations (e.g., ebay, retail stores, online retailers, contest registrations, etc).

Specific guidelines for the appropriate use of electronic mail:

- The use of proper spelling and grammar is expected in all correspondence using the Sumter electronic mail system. The school system promotes academic achievement and a high respect for intellect. All correspondence sent from the school district should reflect these values.
- The sending of mass emails is only appropriate in extremely limited circumstances and only in circumstances that promote the operational and educational goals of the district. It is never acceptable to use the district mail system to sell personal items or business transactions.
- One should not email forwarded personal messages to those that you have not discussed their desire to receive them from you, first. One should limit their forwarding. Forwards containing pictures, sounds & video may be very large files using valuable technology resources and are discouraged.
- **The forwarding of chain letter emails are never appropriate.**
- The district uses technological tools to limit the number of unsolicited junk emails, called “SPAM,” the accounts receive. While this system cannot stop all unsolicited e-mail, it is relatively effective. While much junk mail is sent with no interaction by the recipient, evidence shows that one is far more likely to receive many more such emails if:
- Their email address has been used to register for contests or other marketing techniques on websites,
- Their email address is highly prominent on websites,

- The user sends or receives forwarded messages which have many recipients listed, or
- The user's password is no longer secure or their computer has been infected with malware.

Do not open attachments or follow links from senders you do not know or from whom you are not expecting an email. This is a common method of sending computer viruses, malware, and attempts to gain personal information. Our antivirus and firewall systems delete virtually all virus emails. You may still receive the "disinfected" email but the virus will be replaced with text.

The following practices will increase the effectiveness of E-Mail:

- Make subject headings as descriptive as possible.
- Restate the question or issue being addressed in a response unless the text of the original message(s) is included in the current message.
- Include the most important fact/idea/issue first or very near the top of the message.
- Avoid misunderstandings by keeping in mind that electronic text is devoid of any context clues which convey shades of irony, sarcasm, or harmless humor.
- Limit your forwarding of emails to the most important and be selective to the recipients. Additionally, it is helpful if the sender makes a note to key the recipient in to the important content you wanted to share.
- Proof read/edit each message and use the system's spell check prior to sending a message. You may find it useful NOT addressing the email until AFTER you have proofed the content. This reduces the risk of sending the email prematurely.
- Check the facts in your message before sending it; do not spread rumors via E-mail. Please note stating opinion as fact creates a risk of being accused of libelous communications. Additionally, by forwarding the email, you accept ownership of the email content.
- If you choose to use a background, please be cognizant that dark or excessively busy patterns make emails difficult to read.

Public Records Law Adherence as related to E-Mail:

Most E-mail messages, created or received, in the transaction of official School District business, are public records and open to public inspection according to provisions in Chapter 119, Florida Statutes. Depending on the content and topic of a particular message, it may or

may not be exempt from public inspection under Florida's Public Records Law. **All email correspondence is archived as it is delivered, whether open to public inspection or not. If the user chooses to use the email system for any personal email, you need to be aware that there is no expectation of privacy nor should the district be expected to redact any personal correspondence in response to an open records request.**

Retention Guidelines:

The email system immediately accessible through Outlook or another client, is not intended to be your repository for records retention. District employees are encouraged to delete non-record and transitory messages from their account on a daily basis, immediately after reading, replying, or taking other action concerning a particular message. If the content of an E-mail message possesses long term business value, employees are required to print the message and place it in the proper paper file for further retention or save in a different network location.

Four record categories are described below to assist users in determining the retention requirement of E-mail messages. **It is important to note that an estimated 90% of E-mail messages typically fall under the categories of non-record materials, notices with no business value, or transitory messages and therefore should be deleted by both the sender and receiver immediately after the administrative value is lost.** Please do not use your e-mail account as a replacement for a file cabinet. The email server stores the mail of all users of the system. When this file system gets very large, we are unable to perform much of the maintenance and backup processes necessary for continuous problem-free service.

CATEGORY #1 - Non-Record Materials (delete at will)
The following examples are materials (not records) that may not be appropriate for retention and may be deleted at any time:

- Notice of lost/found items
- Birth/death/funeral announcements
- E-mails not created in the course of School District business Personal mail including forwards and any unsolicited mail

CATEGORY #2 - Notices with No Business Value (delete at will) This category includes information with no business value after receipt and review. Examples include internal office announcements such as:

- "Joe Smith called, please call back"
- "Is this afternoon's meeting still on?"
- "Tomorrow's staff meeting location has been changed to conference room #202."

CATEGORY #3 - Transitory Messages (delete after administrative value is lost)
Transitory Messages consists of those records that are created primarily for the communication of information, as opposed to communications designed for the perpetuation of knowledge. Transitory messages do not set policy, establish guidelines or procedures, certify a transaction, or become a receipt. The informal tone of transitory messages might be compared to the communication that might take place during a telephone conversation or a conversation in an office hallway. Transitory messages would include, but would not be limited to: E-mail messages with short-lived, or no administrative value, voice mail, self-sticking notes, and telephone messages.

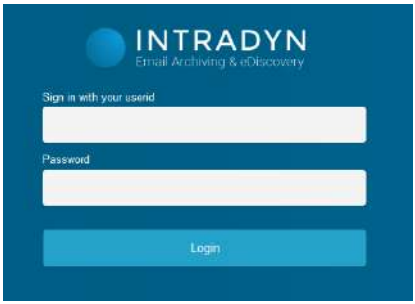
The retention requirement for all transitory messages is "retain until obsolete, superseded or administrative value is lost."

CATEGORY #4 - Official Records (retain as required) E-mail messages that pertain to a particular District business transaction, project/case file, board action, or student/personnel issue must be retained as long as all other documentation that pertains to the same transaction/project/case/action/issue.

Archiving of E-mail Messages

The school district archives all email send and received through the Sumter email system. ***Compliance Vault—RazorSafe*** serves this purpose. Please be aware that the technology department does not have the ability to delete archived mail. If you send personal emails through your district account, it will be archived and could be released through public request for records. While the primary purpose of the ***Compliance Vault*** is for records retention, it is also accessible by users to find old emails that have already been deleted.

To access the ***Compliance Vault***, open a web browser and type in http://razorsafe/ in the address line or select "ComplianceVault Razorsafe" from the Sumter Links Favorites location. Sign in using your network password.



SMART DEVICES

Many, if not most, data devices such as iPhones, Android phones, and tablets, offer data services and are able to connect to corporate electronic mail systems. The district uses Office 365 / Exchange. If your phone supports this technology, you may have the ability to connect to your work email, calendar, contacts, etc. from your personal devices.

1. As a security measure, your device CAN be remotely wiped of data through the Active Sync client by the district. Most, if not all devices will provide an acknowledgement approval message prior to connecting to the Exchange server. The message may contain additional rights to be allowed by the Exchange email system operators. We encourage the careful reading of these terms prior to confirming and connecting to the district's email system.

2. Because various devices have different setup requirements and methods and since there are many possible issues outside our control, district tech services only provides extremely limited support for non-district devices.

3. For security purposes, we anticipate some changes to the process to connect during in the near future. We do anticipate a requirement to be pre-authorized to better protect the network from outside security risks.

4. Settings: Use the following settings to connect your device:

    A) Username: This is your network login name
    B) Password: This is your network password. **Please note, each time you change your network password, it will need to be updated on your device**.

C) Domain: Sumter (depending on your device, this may be asked to be included with your username. If so, separate the domain from the user name with a backslash "\" (e.g. sumter\d09555)

D) Server: **mailman.sumter.k12.fl.us** (many devices prepopulate this field incorrectly when it tries to automatically configure your connection)

E) SSL (encryption) is used, so a field may need to be checked. You may receive a message to accept the certificate or have a checkbox to accept all certificates. It is OK to answer yes or check this as long as you are sure you placed the correct server name.

5. It is the user's responsibility to maintain a reasonable standard of security of their device. Most often this is through a pass code, but at the very least keeping the device physically secure from access by others.

A) Separate the domain from the user name with a backslash "\ " (e.g. sumter\d09555)

B) Server: mailman.sumter.k12.fl.us (many devices prepopulate this field incorrectly when it tries to automatically configure your connection)

C) SSL (encryption) is used, so a field may need to be checked. You may receive a message to accept the certificate or have a checkbox to accept all certificates. It is OK to answer yes or check this as long as you are sure you placed the correct server name.

SOCIAL NETWORKING GUIDELINES

Blogs, social networks and other online tools of publication and commentary, (such as *Facebook, Instagram, Flickr. Google+, Linkedin, Twitter, Snapchat, Vine, Wikipedia, Pinterest, YouTube*, Internet dating, online video games and other similar sites) are new channels for individuals in all walks of life to share information, express creativity and connect with others who have shared interests.

While the district respects the right of free speech of its employees, it is important that all understand that educators are generally held to a higher standard of trust and ethics. These standards can impact the employee in respect to their use of social networking and similar

websites and blogs. All district employees should understand that the use of such sites carries a responsibility of protecting one's personal and professional reputation and not negatively impact their ability to effectively educate the students under their charge.

- In posts, you may identify yourself as an employee, but you must state that you are expressing your own opinion, not that of the district. Your postings will reflect on yourself and the district.
- The Code of Ethics and Principles of Professional Conduct are relevant to all communications, personal and professional.
- Keep it professional - photographs, videos and other materials which might be offensive, could effectively bring your professionalism into question or could reflect attitudes that affect your work with certain individuals and/or diverse groups.
- Posting information that is proprietary or copyrighted, defamatory, libelous, vulgar or obscene may be a violation of federal or state laws, regulations and/or district rules and policies could possibly result in professional and/or personal repercussions.
- Even though you may not have control of what others may post on social networking sites, be aware that your conduct in private life could impact your professional life.
- Please keep a professional distance between yourself and your students. The modern world of social networking opens the door to more situations where separation between your personal life and professional life become more ambiguous and risky for an educator.

Social Media

The District has approved the use of Social Media, (Face Book and Twitter) to communicate with the public at large. Please see the Districts "Social Media Guidelines" for more information regarding the use of Social Media.

STORAGE OPTIONS

One of the benefits to a network is the ability to have special locations to store your files that are backed up on a regular basis. Additionally, the files are also available to you when you use a different computer. **It is imperative that users use the protected file locations and understand that files on a single computer, including the desktop, are transitory and may be deleted without notice due to equipment failure or system updates/upgrades.**

All District accounts are provided with a Office 365 One Drive and access to a school group share drive (often referred to as the “R” drive).

These are provided for the purpose of supporting the district’s mission. They should not be used to store large quantities of files that can easily be replaced or as a location for storage of personal digital photographs or videos. Additionally, all users are responsible for removing their old files when they are no longer relevant.

The district reserves the right to set quotas on the size of one’s user folder or other network storage location.

UNPROTECTED (RISKY) STORAGE LOCATIONS

Your computer’s local hard drive (“C” drive)

This is a temporary location to place extremely large files, such as video and audio files which you can access elsewhere if they are lost. The “C” drive:

- No RAID redundancy as found with server storage
- No backups are made unless the end user creates their own
- Files will be lost upon many technical repairs, updates and upgrades.
- Files do not transfer to a new computer

Your profile’s desktop

This is a convenient location for temporary access to files. Under NO circumstances should original files be placed here without another copy safely located in another storage location. All desktop data remains only on your local hard drive (“C” drive)

- No RAID redundancy as found with server storage
- No backups are made unless the end user creates their own
- Files will be lost upon many technical repairs, updates and upgrades
- Files do not transfer to a new computer

External storage

The use of external storage can provide portable access to files and a location for very large files where space is not available in more protected locations.

- External hard drives provides relatively the same lack of protection as the "C" drive with the exception of the portability increases the chance of loss or physical damage. It is the user's responsibility to create backup copies and provide physical security.

USB "jump drives"

These drives are small and extremely convenient but these benefits also make them more fragile and easy to lose or break.

- Original files should not be stored on this medium. Its purpose is for portability and sharing. The files should always be copied to a protected storage location.
- Due to the ease of loss, NO confidential information should ever be stored on an unprotected USB drive. If temporary storage of protected data is required, the drive must be encrypted.

LOCATIONS FOR MODERATELY PROTECTED STORAGE

- **One Drive.** Your One Drive is only accessible by you, district network administrators or those specifically provided access through the sharing function by the owner. One Drive is housed on Microsoft protected servers and offer a level of redundancy to protect your data.

- **School/Center/District Group Shares (R & J Drives)**

While these locations receive the same physical and backup protections as the most secure, they do allow open access by all with staff rights at the location. <u>This does pose the possibility</u> <u>of another staff member deleting or moving files.</u> **Originals should never be stored in a group share.**

LOCATION FOR THE MOST PROTECTED STORAGE

- **Protected Group Share Locations**. Not to be confused with a school or center's group share (R Drive). These special limited access folders are restricted to specific users, backed up on a regular basis, inaccessible from the internet and protected by anti-encryption technology. All allowed users that have access could conceivably delete file(s) however these folders are backed up and can be restored if notified in a timely manner. This is the safest and most secure storage for data.

ACCESS FILES FROM OUTSIDE THE NETWORK

One Drive files are available anywhere you have a network connection.

INTERNET FILTERING

The district operates a technological tool (iBoss) to filter Internet traffic available within the district. While we respect the free access to information, we also understand the extra care we must follow with our students. The Sumter District Schools remains compliant with the *Children's Internet Protection Act* ***CIPA,*** as required since the district is a recipient of E-Rate funding. If a blocked site is accessed, the user will receive a blocked access web page. If you are blocked from a page that you wish considered to be unblocked information on how can be found later in this handbook.

IMPORTANT: Staff Internet access is covered by different filter rules than student access. Please do not assume a site accessible using your staff account will be accessible by your students. We suggest testing the sites with a class level account with Internet rights. This type of account receives the same filter profile as a student. Staff should not allow students to log on to their laptops as student logons will install an iBoss Mobile device manager on their computer that will limit Staff access to the Internet.

Due to the high volume of network attacks the district receives from outside the US we have turned on GEO Blocking. GEO Blocking means our Firewall rejects traffic from countries other than what we have specifically allowed. If you are unable to open a webpage or receive e-mail from outside the District that you are able to open or receive from your home computer or outside of our network, it has possibly been GEO Blocked. If you believe the website or e-mail source should be allowed please enter a work order to be reviewed.

INTERNET ACCESS AND OTHER USES OF TECHNOLOGY RESOURCES

In general, staff should manage their technology use on a professional basis, keeping the following guidelines and concepts in mind:

- While **LIMITED** personal use of Internet access has been permitted, such personal use should be limited and never occur during the time one is scheduled for face to face instruction. One should not consider their district Internet access to be a replacement for an individual home Internet account.
- No personal business or political use of publicly owned resources is permitted.
- Extra care should be taken as to the appropriateness of the materials accessed or stored on district computers. What may be acceptable in certain environments, may not be acceptable in the school environment.
- The district employs a technological device to limit the likelihood of access to offensive or inappropriate material as required by the *Children's Internet Protection Act (CIPA).* Such filtering is not a replacement for proper supervision and guidance when working with students.
- Bandwidth is a limited shared resource and it is important for the users to be cognizant that their use affects the availability of this limited resource for other purposes.

High bandwidth uses that should be limited include:

- Downloading large files including, but not limited to video, audio and picture files
- Downloading programs
- Streaming media (watching online video, listening to online audio)
- Online games and animation
- Syncing devices, such as iOS & Android through iTunes, Google Play, Amazon Market, etc.
- Personal pictures, video or audio files should not be stored on district servers (i.e. user folders, share drives, etc.)
- Temporary sharing of a few personal event pictures, i.e. births, weddings, etc., are acceptable as long as they are removed in a timely fashion (less than one week).

Such uses should always be limited to educational needs and preferably before 8:00 am or after 3:00 pm.

1 to 1 TAKE HOME LAPTOPS

Students and Staff that are issued laptops to take home are required to make sure their laptops have active and up to date Kaspersky on them,

that windows updates are being applied on a regular basis and that the laptop remains in good working order.

- All issued laptops should be brought to school every day.
- Windows updates are automatic but the computer must be turned on for updates to be downloaded and applied.

STUDENT USE OF TECHNOLOGY

Technology resources provide promising opportunities to enhance the educational experience for students. Bringing access to libraries and museums, providing sophisticated tools and providing instructional tools for sophisticated tracking and feedback systems. For the tools to be successful, it is the teacher's responsibility to use them appropriately and efficiently; improper use can actually create an environment that interferes with the instructional process. Keys to proper and effective use of technology:

- It is important that teachers become proficient in the technological tools being used in the instructional process. Additionally, online sites are to be visited prior to class use to verify that they can be accessed and are appropriate to the lesson. If the students are expected to visit the sites under their logon, one needs to verify the site is available under a student filtering profile. The easiest way to accomplish this to visit the site(s) using a "class" account.
- Technological based courseware and other applications provide the teacher with tools for data analysis and student assessment. It is important that teachers use this data to make adjustments as necessary to meet the instructional needs of the students.
- It is extremely important to monitor student online activities to make sure students are on task and meeting the objectives of the class. Proper classroom management is paramount for effective use of instructional technology.
- Most people find the expanse of information on the Internet overwhelming. Assisting students with proper searching techniques as well as the means to evaluate sources is extremely important to make learning productive.
- Technology not only provides access to information, it also allows for easy means to plagiarize the works of others. Teachers need to be diligent to assist students in understanding the importance of copyright and citing sources.

- Student safety while online is an important aspect of our preparation of students to be safe and become productive members of society.

The *Children's Internet Protection Act (CIPA)* sets specific monitoring requirements for school districts to provide student access to communication services, such as e-mail. Depending on how used, wikis, blogs and other *Web2.0* media may also have special requirements.

Student email is available to all students through Office 365. Due to CIPA and requirements of the Acceptable Use Policy, the only supported email addresses for students are provided by the district. In order to remain compliant with CIPA, it is important that school staff encourage the use of this account for school work instead of their personal accounts. The system being utilized provides filtering and monitoring capabilities as required by *CIPA.* Access may require monitoring to be done by the teacher. *Office 365* is accessible from school and home where consumer email services are not available from school.

STUDENT INTERNET SAFETY

As part of preparing students for our technological world, it is important that we integrate Internet safety into our instructional process. Congress added additional requirements for schools to instruct students in Internet safety, particularly in safely understanding the use of social media. Additionally, School Board policy requires schools to provide Internet safety instruction.

According to *i-Safe America*, the World Wide Web has become a playground for millions of youth who are at risk of exploitation and abduction by predators seeking to cloak their identity and motives. For teens, the Internet has become their primary communication tool, even surpassing the use of the telephone. Consider just a few Web facts:

- 1 in 4 children age 10-17 have been exposed to pornography.
- 1 in 5 children under age 17 have received unwanted sexual solicitation.
- 1 in 33 children have received an aggressive solicitation to meet somewhere.

Students should be taught that:

- Guarding their identifying information (name, sex, age, address, school, teams) is of upmost important. It only takes a little information for a predator to identify you.
- Responsible adults do not pursue relationships with kids and teens.
- Cyber-Bullying is wrong and harmful to others
- Materials distributed/posted may be shared by others without their knowledge making it virtually impossible to remove all incidences of such materials
- Under the *Children's Online Privacy Protection Act* (COPPA), websites are not allowed to collect personal data from people under the age of 13 without a parent's permission.
- Certain inappropriate acts may be illegal, including but not limited to what is commonly referred to as "sexting."
- Their usernames should be generic and anonymous.
- Their online profiles are generic and anonymous.
- Attachments and links in e-mails from strangers can contain Viruses and other risks.
- Pictures are great to hand to a friend, but it's not cool to send them to an Internet "friend."
- Posting your picture on the Internet gives hackers the chance to doctor your picture and make fun of you to everyone on the World Wide Web.
- Chat room "friends" are not always who they say they are.

I-Safe America is a non-profit foundation whose mission is to educate and empower you to safely and responsibly take control of their Internet experience.

COPYRIGHT AND LICENSING OF ELECTRONIC MEDIA

The Sumter District Schools recognizes the importance of the Copyright Law in the United States (Title 17, United States Code) and expects all its students and staff to abide by the law. School Board Policy 2531 addresses Copyright compliance.

With the wide access to the Internet, information has become readily available and easily duplicated. The fact of easy copying does not reduce the copyright owner's rights to their property.

As a general guideline,

- Assume materials have all rights reserved, unless otherwise indicated.

- Follow fair use precedents and guidelines as you would with other materials
- Look for rights under *Creative Commons* when possible
- Properly cite all sources, whether found through the Internet or available in other means
- Request permission when in doubt

Most programmed technologies are licensed for use, whether purchased or provided at no charge. It is imperative that the rights and restrictions as stated in the licensing agreements are respected and followed.

When accessing or downloading materials you are likely to receive a *Terms of Service* document to accept. You are encouraged to read this document since you and your students are bound by these Terms of Service.

Know the rules about Intellectual Property. Do not illegally download music and movies.

The district uses *Copyright: A Guide to Information and Resources* by Gary H. Becker as its general guide to Copyright Law. This material should be readily available through your school library media center.

COMPUTER USE, SAFETY AND COMFORT

1. Don't sit in one fixed posture for long periods of time. Avoid slouching forward or leaning back too far.
2. Avoid placing boxes or other items under your desk that limit your leg room. You should be able to pull yourself all the way up to your desk without interference.
3. Remember to stay relaxed particularly in areas where muscle tension often builds, such as your shoulders.
4. While looking at your monitor and also while resting your eyes, remember to blink. This helps keep your eyes naturally protected and lubricated and helps prevent dryness. Give your eyes frequent rests by focusing them on a distant point.
5. If you wear bifocals or trifocals, don't position your monitor so high that you have to tilt your head back to view the screen.
6. Don't position your keyboard and pointing device at different levels and distances.
7. Avoid gripping or pinching your mouse tightly.

8. Don't arrange your work area in a way that causes you to repeatedly strain forward to see and reach frequently used items such as books, papers, or a phone.
9. Insure that slots and openings in electronic devices are open to allow proper ventilation to maintain temperature control.
10. Use surge protection power source for computer hardware when possible and do not overload electrical circuits.

ENERGY AND NATURAL RESOURCE EFFICIENCY

The Sumter District Schools uses energy management processes that have shown a considerable cost avoidance. Through this rigorous effort, the district has been awarded the designation of an Energy Star Partner. (www.energystar.gov) The Technology Department supports reasonable means to reducing electricity and other energy uses while not over-taxing the equipment or limiting the positive aspects of technological implementations.

- **Turn off all computers, monitors and peripherals at the end of the work day.** Be aware that even when devices are in a "sleep" mode, they pull some electricity.
- Screensavers do not save electricity. **During the day, the computers are set to turn off the monitor after a period of inactivity**.
- **Power off video projectors when not in use**. This saves not only electricity, but lamp life. An LCD projector lamp will last approximately 2000 hours and can cost over $200 to replace,
- Allow for **adequate equipment ventilation** for cooling by keeping slots, openings and fan exhaust open. Since most of our computers have thermostatically controlled fan speeds, a clean computer is likely to run, not only cooler, but quieter.
- The equipment in server rooms must run 24/7, so it requires temperature control at all times. Since the exhaust temperature on a server is typically 15-20 degrees above the intake, **Server room temperatures should never exceed 80 degrees**.
- One can save substantially by **limiting printing** whenever possible. This not only saves electricity, but paper and toner costs. Electronic documents are intended to be read in their electronic format.
- Due to turning off computers after hours and all summer, users need to be aware that updates and virus scans run during work

hours and may affect the speed of the computer. You can reduce this situation by:

- Logging computers on before students are present
- Using all computers regularly - Computers that are only used occasionally will have more updates awaiting installation
- Planning extended update times before students return after holiday breaks, particularly summer and winter.
- All computers, including laptops at a minimum, should be turned on, rebooted on the network at least once a week to ensure Anti-virus and Windows updates are current.

BOARD POLICY 7540.04

7540.04 - **STAFF TECHNOLOGY ACCEPTABLE USE AND SAFETY**

Technology has fundamentally altered the ways in which information is accessed, communicated, and transferred in society. As a result, educators are continually adapting their means and methods of instruction, and the way they approach student learning, to incorporate the vast, diverse, and unique resources available through the Internet. The School Board provides technology and information resources (as defined by Bylaw 0100) to support the educational and professional needs of its staff and students. The Board provides staff with access to the Internet for limited educational purposes only and utilizes online educational services/apps to enhance the instruction delivered to its students and to facilitate the staff's work. The District's computer network and Internet system do not serve as a public access service or a public forum and the Board imposes reasonable restrictions on its use consistent with its limited educational purpose.

The Board regulates the use of District technology and information resources by principles consistent with applicable local, State, and Federal laws and the District's educational mission. This policy and its related administrative procedures, Policy 7544 and any applicable employment contracts and collective bargaining agreements govern the staff's use of the District's technology and information resources and staff's wireless communication devices when they are connected to the District's computer network, Internet connection, and/or online educational services/apps, or when used while the staff member is on Board-owned property or at a Board-sponsored activity (see Policy 7530.02).

Users are required to refrain from actions that are illegal (such as libel, slander, vandalism, harassment, theft, plagiarism, inappropriate access, and the like) or unkind (such as personal attacks, invasion of privacy,

injurious comment, and the like). Because its technology resources are not unlimited, the Board has also instituted restrictions aimed at preserving these resources, such as placing limits on the use of bandwidth, storage space, and printers.

Users have no right or expectation to privacy when using District technology and information resources (including, but not limited to, privacy in the content of their personal files, e-mails, and records of their online activity when using the District's computer network and/or Internet connection).

Staff members are expected to utilize District technology and information resources to promote educational excellence in our schools by providing students with the opportunity to develop the resource sharing, innovation, and communication skills and tools that are essential to both life and work. The Board encourages the faculty to develop the appropriate skills necessary to effectively access, analyze, evaluate, and utilize these resources in enriching educational activities. The instructional use of the Internet and online educational services will be guided by Board Policy 2520 - Selection of and Adoption of Instructional Materials.

The Internet is a global information and communication network that brings incredible education and information resources to our students. The Internet connects computers and users in the District with computers and users worldwide. Through the Internet, students and staff can access relevant information that will enhance their learning and the education process. Further, District technology resources provide students and staff with the opportunity to communicate with other people from throughout the world. Access to such an incredible quantity of information and resources brings with it, however, certain unique challenges and responsibilities.

The Board may not be able to technologically limit access, through its technology resources, to only those services and resources that have been authorized for the purpose of instruction, study, and research related to the curriculum. Unlike in the past when educators and community members had the opportunity to review and screen materials to assess their appropriateness for supporting and enriching the curriculum according to adopted guidelines and reasonable selection criteria (taking into account the varied instructional needs, learning styles, abilities, and developmental levels of the students who would be exposed to them), access to the Internet, because it serves as a gateway to any publicly available file server in the world, opens classrooms and students to electronic information resources that may

not have been screened by educators for use by students of various ages.

Pursuant to Federal law, the Board has implemented technology protection measures that protect against (e.g., filter or block) access to visual displays/depictions/materials that are obscene, constitute child pornography, and/or are harmful to minors, as defined by the Children's Internet Protection Act (CIPA). At the discretion of the Board or Superintendent, the technology protection measures may also be configured to protect against access to other material considered inappropriate for students to access. The Board also utilizes software and/or hardware to monitor online activity of staff members to restrict access to child pornography and other material that is obscene, objectionable, inappropriate, and/or harmful to minors. The technology protection measures may not be disabled at any time that students may be using the District technology resources if such disabling will cease to protect against access to materials that are prohibited under the CIPA. Any staff member who attempts to disable the technology protection measures without the express written consent of an appropriate administrator will be subject to disciplinary action, up to and including termination.

The Superintendent may temporarily or permanently unblock access to websites or online educational services/apps containing appropriate material, if access to such sites has been inappropriately blocked by the technology protection measures. The determination of whether the material is appropriate or inappropriate shall be based on the content of the material and the intended use of the material, not on the protection actions of the technology protection measures. The Superintendent may also disable the technology protection measures to enable access for bona fide research or other lawful purposes.

Staff members will participate in professional development programs in accordance with the provisions of law and this policy. Training shall include:

A. the safety and security of students while using e-mail, chat rooms, social media, and other forms of direct electronic communications;

B. the inherent danger of students disclosing personally identifiable information online;

C. the consequences of unauthorized access (e.g., "hacking", "harvesting", "digital piracy", "data mining", etc.), cyberbullying,

and other unlawful or inappropriate activities by students or staff online; and

D. unauthorized disclosure, use, and dissemination of personally identifiable information regarding minors.

Furthermore, staff members shall provide instruction for their students regarding the appropriate use of technology and online safety and security as specified above, and staff members will monitor students' online activities while at school.

Monitoring may include, but is not necessarily limited to, visual observations of online activities during class sessions or use of specific monitoring tools to review browser history and network, server, and computer logs.

The disclosure of personally identifiable information about students online is prohibited.

Building principals are responsible for providing training so that Internet users under their supervision are knowledgeable about this policy and its accompanying procedures. The Board expects that staff members will provide guidance and instruction to students in the appropriate use of the District technology resources. Such training shall include, but not be limited to, education concerning appropriate online behavior, including interacting with other individuals on social media, including in chat rooms and cyberbullying awareness and response. All users of District technology resources are required to sign a written agreement to abide by the terms and conditions of this policy and its accompanying procedures.

Staff will be assigned a school email address that they are required to utilize for all school-related electronic communications, including those to students, parents and other constituents, fellow staff members, and vendors or individuals seeking to do business with the District.

With prior approval from the Superintendent, staff may direct students who have been issued school-assigned email accounts to use those accounts when signing-up/registering for access to various online educational services, including mobile applications/apps that will be utilized by the students for educational purposes under the teacher's supervision.

Staff members are responsible for good behavior when using District technology and information resources - i.e., behavior comparable to that

expected when they are in classrooms, school hallways, and other school premises and school sponsored events. Communications on the Internet are often public in nature. The Board does not approve any use of its technology and information resources that is not authorized by or conducted strictly in compliance with this policy and its accompanying procedures and Policy 7544 and its accompanying procedure.

Staff members use of District technology resources to access or use social media is to be consistent with Policy 7544 and its accompanying procedure.

An employee's personal or private use of social media may have unintended consequences. While the Board respects its employees' First Amendment rights, those rights do not include permission to post inflammatory comments that could compromise the District's mission, undermine staff relationships, or cause a substantial disruption to the school environment. This warning includes staff members' online conduct that occurs off school property including from the employee's private computer. Postings to social media should be done in a manner sensitive to the staff member's professional responsibilities.

General school rules for behavior and communication apply.

Users who disregard this policy and its accompanying procedures may have their use privileges suspended or revoked and disciplinary action taken against them. Users are personally responsible and liable, both civilly and criminally, for uses of District technology and information resources that are not authorized by this policy and its accompanying guidelines.

The Board designates the Superintendent as the administrator responsible for initiating, implementing, and enforcing this policy and its accompanying procedures as they apply to staff members' use of District technology and information resources.

In addition, Federal and State confidentiality laws forbid schools and their employees from using or disclosing student education records without parental consent (see Policy 8330). Education records include a wide variety of information; posting personally identifiable information about students is not permitted. Staff members who violate State and Federal confidentiality laws or privacy laws related to the disclosure of confidential student or employee information may be disciplined.

Staff members retain rights of communication for collective bargaining purposes and union organizational activities.

TELEPHONE SYSTEM

All schools/sites are served by a single Cisco phone system that functions on the computer network. The telephone system offers many features, most notably, most staff have access to voicemail, even if they do not have a telephone on their desk. Voicemail is not only delivered to the telephone extensions, but also to one's email.

Also, the entire district is part of the same phone "network", you can dial any extension from any location.

Extensions are 5-digits with the first two representing the location:

BES 63xxx	SSMS 71xxx
WES 64xxx	WMHS 81xxx
WWE 62xxx	SSHS 82xxx
LPES 61xxx	SAS 83xxx
CO 50xxx	SPC 51xxx
TRANS 53xxx	FAC/FS 52xxx

Additionally, extensions are coordinated to certain positions to assist in dialing. For example:

Front Desk xx200	Cafeteria xx221
School Secretary xx201	Head Custodian xx224
Principal xx210	Data Entry xx203
Media Center xx220	Guidance xx23x

An instructional video on the 6900 series phones can be found at:
http://goo.gl/mZKX7C
6900 Series Quick Start Guide: http://goo.gl/RZIDgh

TECHNICAL PROBLEM? HOW TO GET ASSISTANCE

Technical Problem or Question?

Collect pertinent information.

- Computer Name/Number
- User whose account the issue occurred
- Gather as much information as you can (error message, applications running, etc.)

Call Support
(352) 793-2315 ext 50250

Or email:
Support@sumter.k12.fl.us

Or complete a work order.
Look in your Favorites under *Sumter Links*

http://sco-servicedesk:8081/