ELECTRONIC COMMUNICATION POLICY

The School Board's computer, telephone, and other electronic equipment are provided to employees to permit our organization to provide better service and to facilitate more efficient communications internally. The School Board's E-mail, telephone and voicemail systems belong to the School Board and should be used only for School Board business. Confidential information shall be preserved and shall not be disclosed or disseminated to those who do not have a legitimate need to know. Employees' private E-mail and voicemail messages not related to School Board business should not be placed on the E-mail or voicemail system. Employees should direct personal mail and telephone calls to their non-work devices to the extent possible and practicable.

1. **Prohibited Use of Electronic Systems and Devices**

   Employees are prohibited from using School Board computers, the mail or other electronic communication systems or company or personal devices to:

   - Send or receive messages or files that are illegal, sexually explicit, abusive, offensive or profane, disruptive, discriminatory, harassing or threatening.
   - Access the Internet other than for legitimate business purposes.
   - Disclose personal, confidential information, copyrighted materials, intellectual property to unauthorized recipients.
   - Engage in the use of electronic systems for purposes of “snooping."
   - Secretly record any conversation in the workplace.
   - Intercept or review electronic communications not addressed to you without authorization.
   - Encrypt email or files with the use of software not approved by the School Board.
   - Engage in any illegal or wrongful conduct.
   - Download or load unauthorized software and/or download or load software or files without complying with established policies to check all such software for computer viruses that could disrupt performance of the system.
   - Use passwords or encryption for the purpose of limiting School Board access.

2. Monitoring and Privacy

The School Board treats all messages, files and telephone conversations sent, received, or stored in the electronic and voice communication systems as School Board messages. The School Board may access, review, record, copy, disclose and delete any messages, blogs, tweets, communications, or files sent, posted, received or stored on the electronic and voice communication systems, and may periodically, on an announced or unannounced basis, access, review, copy, disclose and delete messages, , blogs, tweets, communications, or files received or stored on the systems to ensure that the systems are working properly, that no viruses have been introduced, and that all employees are abiding by this policy. THERE SHOULD BE NO EXPECTATION OF PRIVACY ON THE PART THE EMPLOYEE USING THE SCHOOL BOARD'S COMPUTOR, TELEPHONE, OR ELECTRONIC SYSTEMS. Employees should not use the School Board's computer, telephone, or electronic systems to post, send, receive or store any material that they wish to keep private.

3. Disciplinary Consequences for Violation of This Policy

Violation of the School Board's Electronic Communications Systems policies is prohibited and subject to disciplinary action, up to and including termination.

Acceptable Use Policy (AUP) for Electronic Resources Implementation Guidelines (Employees)

Table of Contents

Expected Behaviors

These guidelines are in effect seven days a week, 24 hours a day, for use anywhere on the school board's network and/or with school board electronic resources. Individual users shall at all times be responsible for the proper use of accounts issued in their names.

Do

Employees shall:

1. Be familiar with the AUP and Implementation Guidelines.

2. Use electronic resources for educational purposes, such as:
   - Lesson planning,
   - Classroom instruction,
   - Research,
   - Professional development,
   - Collaboration with peers,
   - Participation in global learning communities, and
   - Communication with experts.

3. Check school board provided email frequently and delete unwanted or unneeded messages promptly.

4. Keep passwords private and change them frequently.

5. Follow Netiquette rules.

6. Make back-ups of important data files.

7. Report any security problems, errors, bugs, viruses, system weaknesses, or damage to an immediate supervisor.

8. Report any inappropriate message, or other communication that makes a student or employee feel uncomfortable, to an immediate supervisor.

9. Log off when leaving a computer station.

Don't

In addition to those activities prohibited in the Acceptable Use Policy, employees shall not:

1. Use another person's username and password or allow someone else to use theirs.
2. Leave user accounts open or unattended.
3. Send or spread viruses or other harmful software.
4. Broadcast uninvited messages ("spamming") or send chain letters.
5. Use obscene or offensive language.
6. Download, copy, and/or share software, videos, music, movie files, or anyone else's work for which educational use rights have not been granted as per Copyright Law.
7. Enter and/or damage another person's folders, work or files.
8. Damage or attempt to damage the network, equipment, materials or data.
9. Access any electronic resource without proper authorization.
10. Monopolize equipment, bandwidth, storage space or any other shared resources.
11. Use the network for video or audio entertainment.
12. Download or install any software without authorization.
13. Use electronic resources for illegal activities such as, but not limited to, the illegal sale or illegal use of drugs or alcohol, participation ~~I~~in or facilitation of criminal gang activity, participation in or facilitation of gambling.
14. Alter, disable, or remove the Santa Rosa County School Board Acceptable Use Policy notice presented at login, as a screen saver, or in another form.

Important Information for Employees:

Users should have no expectation of privacy in any communication sent or received by email, or in regard to the Internet, network access, or other electronic resources. This also applies to files that are archived or otherwise recoverable. School officials may review files and communications to ensure that users are using the system responsibly.

Use of Electronic Resources

Santa Rosa County School Board electronic resources are primarily for educational use. Any information carried or contained on these resources is subject to review.

Personal Devices

Employees may not use a personal electronic device to access any school's local area network (LAN) and/or the school board's network, or any information contained or stored in electronic resources, without specific permission from school or school board technology staff. Devices used solely to attach to SR Connected wireless network do not require prior approval but must serve an educational purpose. If any such electronic device is installed or connected, its use and all information and data on it shall be subject to the policies of the school board and any additional school or district department guidelines.

Employees wishing to use personal computers and/or personal mobile devices on the network (e.g., iPads) must request permission to connect to the network from the TSA Supervisor or designee. Once approved for network access, Internet use will be monitored via the district content filter and access secured through the district Airtight security appliance. Additional permission to use unfiltered, third-party networks (e.g., 3G or 4G) is required from the site administrator and the TSA Supervisor or designee. Under no circumstances should an unfiltered, third-party network be used in an instructional setting where students are present.

Instructional use of personal wireless devices (i.e., iPads and similar tablet-like devices) beyond the administrative scope mentioned in the section "District-Owned iPads and Other Tablet Devices" is also currently being evaluated. Filtered wireless access, known as SR WiFi, may be made available to staff for instructional purposes. This network allows access to Santa Rosa Domain resources. All 802.11x Wireless devices (non 3G/4G) that access the iBoss-filtered SR WiFi wireless network must be approved and authorized through the AirTight security appliance before use on School Board property.

Formatted: Highlight

An additional filtered wireless access, known as "Santa Rosa Connected" (SR), ~~will soon be~~ is available to students and others in Media Centers and schools across the district. This filtered wireless network does not allow access to SR domain resources. This initiative intends to engage students, improve access, foster creativity, increase the integration of technology into the curriculum, promote higher level thinking skills, and ultimately improve achievement. All 802.11x personal devices (non 3G/4G) that access the SR Connected wireless network will be limited to iBoss Filtered Internet access only but will not require authorization through the AirTight security appliance. Refer to Student Mobile Device Use and SR Connected District Policy (https://www.santarosa.k12.fl.us/pdc/docs/)

These wireless networks are new technology for the school district, and the impact on the district infrastructure and support systems has yet to be determined. Requests for teacher and/or student use of wireless devices on SR Connected for instructional purposes should be made to the site administrator.

Formatted: Highlight

Hardware and Purchasing of Electronic Resources

Any device or application that interacts with the school/district network must serve an educational purpose and be approved prior to purchase, installation, or use. Devices used solely to attach to SR Connected do not require prior approval but must serve an educational purpose.

Form 63-11-53A (https://www.santarosa.k12.fl.us/pdc/docs/) must be submitted to ~~a Technical Support Software Technician (see form for specific technician)~~the staff member specified on the form error-checking and further processing. Certain requests may be evaluated by the District Technology Committee or its designees.

District-Purchased Hardware

The Technical Support Annex (TSA), working in conjunction with the Professional Development Center (PDC), has the responsibility for determining the hardware standard configuration for administrative and instructional computers and servers. Data Processing will work with the Purchasing Department to ensure adherence to district policies and procedures for the hardware bid process and vendor selection. Only hardware purchased through district-approved hardware vendors will be technically supported. This includes laptops/tablet PCs, handheld devices, printers, and scanners approved and provided through the District's selected vendor(s).

Formatted: Highlight

Any device NOT obtained through this process nor previously approved by the TSA Supervisor will not be maintained by the Technical Support technicians and will require the purchase of warranty support from the vendor. No district standard is set for digital cameras, video cameras, or peripheral equipment (excludes printers and scanners). Purchase and support of these items are school-based decisions and responsibilities. The Department of Exceptional Student Education and Data Processing will support Assistive and Adaptive equipment required by Individual Education Plan (IEP) specifications.

Formatted: Highlight

All staff laptops that attach to the district network must have a district-approved operating system and virus protection software installed. Laptops may be used as teachers' school workstations. Laptops – set up and purchased through the District – may be used at home for work-related purposes, but the district will not support Internet access at home (though the district's ghost image will not be configured to prevent home Internet access).

Under no circumstances are students to physically connect to any port or district-owned device while on School Board property through Ethernet cables, USB cables, Paralink cables, etc., or to connect by Ad Hoc mode to any other district-owned device.

All schools should address obsolete hardware replacement in their school-based technology plans. A district plan is in place to update school-based computers. Data Processing will be responsible for replacement of administrative hardware. The Professional Development Center is responsible for replacement of district (PDC) training lab hardware.

Formatted: Highlight

No acceptance of free hardware offers from vendors or individuals may be made without approval of the Director of Instructional Technology and the Data Processing Manager. Approval will be based on an examination of the requirements for receipt of the equipment, the nature of the use of the equipment and the maintenance requirements. No equipment or product that uses ads from corporate sponsors to pay for the products will be approved.

Donated hardware from business partners, parents, community businesses, the military or district employees should be consistent with the current minimum configuration. The District will not support donated hardware that hasn't been pre-approved for support by DP and PDC. Schools should confer with the Director of Instructional Technology or the Data Processing Manager prior to accepting any donated hardware. Prior to the issuance of a contribution letter for tax purposes, school principals should work with Data Processing to determine a fair market value as required by federal IRS regulations.

Formatted: Highlight

To meet safety regulations, the mounting of LCD projectors and other technologies (that require mounting) in district buildings/classrooms must be done by district-contracted professionals. Please see the district w~~W~~eb Documents & Forms page for the latest Approved Projector and Installation Purchasing Information.

District-Owned iPads and Other Tablet Devices

The district ~~is in the process of implementing~~ has implemented administrative-level use of iPads for Teacher Observation and Evaluation. All use will comply with the State Board of Education Rule 6B-1.006, FAC The Principles Of Professional Conduct Of The Education Profession In Florida (Code of Ethics). The Technical Support staff will set up and activate these wireless devices, the use of which will be monitored via the district content filter and access secured through the district Airtight security appliance. Other school- or district-purchased iPads will follow the same process. Additional permission to use unfiltered, third-party networks (e.g., 3G or 4G) is required from the site administrator and the TSA Supervisor or designee. Under no circumstances should an unfiltered, third-party network be used in an instructional setting where students are present. Policy for student use of these devices is ~~currently being written~~available on the district Documents & Forms page (see Student Mobile Device Use).

~~Instructional use of wireless devices (i.e., iPads and similar tablet-like devices) beyond the administrative scope mentioned above is currently being evaluated. This is new technology for the school district, and the impact on the district infrastructure and support systems has yet to be determined.~~ Requests for teacher and/or student use of approved wireless devices for instructional purposes should be made to the site administrator and if approved forwarded to the TSA Supervisor for final approval and authorization of setup.

Tablet devices issues by the Santa Rosa District School Board are subject to the same policies and procedures of non-portable devices. No personal use of these devices is appropriate. Employees should use tablet devices in accordance with job duties and assignments.

iPad setup requires users to have an iTunes account. This account requires an electronic payment method and an email account. To avoid potential discrepancies, a personal email account and payment method should be used. In the event that school purchases are made on the iPad, the employee may enter the district credit card information as payment. iPads should be Passcode locked and set to Auto-lock in 5 minutes or less.

The use of a modem on school board property requires specific permission from the Technical Support Annex (TSA) Supervisor.

Removing/Borrowing Equipment

Employees may remove equipment from school board property when necessary to accomplish tasks associated with position responsibilities. In order to remove equipment from school board

property, employees must follow appropriate procedures as outlined by each school district department, including sign-out forms with acknowledgement of liability for loss or damage.

Limits on Use of Resources

The maintenance, monitoring and regulation of the District's network resources are the primary responsibilities of the Manager of Data Processing and the District communications operator. Bandwidth expansion will be determined based on need and usage.

Employees must exercise great care in the use of electronic resources. The network is not designed for video or audio entertainment. The following will help avoid network gridlock:

a. Users should not tie up the network with idle activities such as surfing the Internet or playing games.

b. Users should limit the use of streaming video and audio to ensure that there is sufficient bandwidth to support other educational activities. Be aware that although streaming video and audio may appear to be basic uses of the Internet, they consume large amounts of bandwidth (network resources).

Due to bandwidth concerns, all Internet-based curriculum resources must be approved by the ~~Technical Support Department~~ Data Processing prior to purchase. Examples of online curriculum resources include: *Discovery Education Digital Media; Accelerated Reader Enterprise; Worldbook Online;* and online periodicals.

Formatted: Highlight

The use of MP3, MVI, and similar file structures for both audio and video must be in support of educational activities, limited to very specific project needs, and in keeping with bandwidth restrictions and copyright considerations. Student use of these types of files will be conducted under the guidance of a faculty member.

Troubleshooting/Repairs

While it is expected that employees apply basic trouble-shooting techniques (checking power cords, cables, etc.) users shall not attempt to repair electronic resources. All requests for repair or service must be forwarded to the appropriate school technology contact. At all non-school sites, all requests for repair or service must be forwarded to school board support personnel via the Data Processing Help Desk or work order system.

Software

The Data Processing department, in consultation with the Professional Development Center, sets administrative software and operating system standards. Training on the standard production and operating system software will be provided by the PDC.

Instructional software standards will be set by the Professional Development Center in consultation with Data Processing, schools and the District Technology Committee. The District Network **Software Analysts will support only software approved prior to purchase** by the Director of Instructional Technology. **The PDC will make every effort to test or pilot any proposed software purchases.** Software training will be provided by the PDC on any district-wide approved/adopted products. The District trainers will not provide training for products purchased by individual schools unless such arrangements were made prior to the purchase.

Prior to any large-scale software installations, school Technology Contacts are encouraged to seek guidance from district Network Analysts.

The purchase and loading of approved, stand-alone software on district computers will be at the discretion of the school-based administrator and technology contact (see the Approved Instructional Software list at https://www.santarosa.k12.fl.us/pdc/docs/). Software not currently on the approved software list must be submitted to TSA or PDC for approval via Form 63-11-53 "Request For New Technology Approval." Approval must be obtained prior to the loading of any such software. Any personal software brought from home to be loaded on district computers requires complete licensing agreement paperwork as well as completion of Form 63-11-38 "Request for Software Installation/Use" or Form 63-11-53 if not already on the approved list. **Note**: The software becomes the property of the school district once loaded on district hardware.

The District's standard virus protection software must be loaded on all computers that access the District network; this includes those personally owned by employees and contracted services (i.e., laptops). Vendor laptops must be checked for up-to-date antivirus software prior to connection to the District network (SR Connected (SR) should be used for vendors, if available.)

On student workstations, it is required that the district-approved operating system be configured to restrict access solely to educational applications. Student workstations must be configured to prohibit student administrative access.

The District lacks the resources to support stand-alone software/apps purchased by teachers or schools from local vendors. Schools should exercise greater caution when purchasing and loading stand-alone software from non-educational software providers.

Reinstallation of Software/Data Files

On occasion it is necessary that school and/or school board technology personnel reformat hard drives or other storage devices. Reformatting completely erases all contents of these devices. All school board software which is consistent through the district, such as *Microsoft Office*, will be reinstalled. All other approved software will need to be reinstalled by school educational Technology Contacts and/or network specialists once proof of licensing has been obtained. Unapproved copies of software will not be reinstalled, nor will personal data files be restored. Please keep any installation disks of specific school-purchased software in an identified location on campus should the need for reinstallation arise. Please be personally responsible for making backups of any important data files that are stored on local hard drives.

Wireless

In order to ensure the security of the network, implementation of wireless connectivity (following 802.11 or newer standards) at any district site must follow district wireless standards (e.g. Enterprise wireless components). Each implementation of wireless devices much be approved by the TSA Supervisor or manager prior to acquisition.

Structured Cabling

All retrofitting and equipment upgrades should be done in collaboration with Data Processing and the District-approved contractors. Any district-supported retrofitting projects will be done with collaboration among the Director of Instructional Technology, Data Processing, the District-contracted engineering firm, the District's cable vendor, and the school principal or

designee. All structured cabling projects must follow the District- approved standards as specified and updated yearly in the District Technology Plan.

All requests for computer cabling will be submitted to the Data Processing Department, using either a Data Processing Work Order or email. Once the request is received by Data Processing, the Technician Supervisor will schedule a walk-through with the current cabling contractor. The contractor will supply a price to be reviewed by data processing then forwarded to the school or department.

If the cabling is for instructional purposes, the school will submit a request for PO, including all items as listed on the quote. All cabling must be approved by the Data Processing Manager and the Director of Instructional Technology or their designees.

If the cabling is for administrative purposes, data processing will handle the paperwork.

The following timeline will be the goal for the entire cabling process.

- School sends work request to DP
- Work Order is approved 2 days
- Cabling contractor is called & walkthrough is performed 2 days
- Contractor provides quote 3 days
- School is provided with the quote 2 days
- Site initiates request for PO 1-5 days
- Work is completed after receipt of purchase order 10 days

Support

Support for all administrative hardware and software is the responsibility of the Data Processing Department. Data Processing will maintain technicians who will install and support all district standard hardware and software used for administrative purposes.

Instructional Technology support is the responsibility of the Professional Development Center and Data Processing. Work orders for any software or hardware technical support must be submitted through the District's work order system. Data Processing will assign hardware and software work orders to the appropriate technician. Technicians will attempt to address work orders in chronological order. Often, however, jobs must be prioritized otherwise due to district goals or the number of students being affected by an issue. The Professional Development Center and the Data Processing technicians will work together to resolve technical work orders as soon as possible.

The District supports the following major network software applications:

A3
Accelerated Reading/Math
Classworks Gold
Discovery Education Assessment/Streaming
Earobics
Excelsior Grade 2 (until Fall 2012)
My Reading Coach
Peachtree Accounting
Read 180
Reading Counts
Renaissance Learning
Rosetta Stone

FASTT Math	S4
Follett/Destiny	SchoolStream
Imagine Learning English	SMART2
Microsoft Office Suite (~~2003/~~2007/2010/2013)	SuccessMaker Enterprise™
Microsoft Server (~~NT/2000/~~2003/2008/2012)	Vantage Writing
Microsoft Windows OS (~~XP/~~7)	Writer's Solution

Other software applications will be examined and added as needed. For additional approved software please refer to Addendum 7A – Instructional Software (https://www.santarosa.k12.fl.us/pdc/docs/)

Internet Guidelines

Because the Internet is a widely-used instructional tool, it is important to continually evaluate its use. The District will provide content filtering software for the safety of our students. Under the current Child Internet Protection Act (CIPA), districts receiving federal technology dollars through E-rate or various technology grants must provide Internet filtering software and must ensure that all students receive instruction related to appropriate online behavior, including interacting with other individuals on social networking sites and in chat rooms, and Cyberbullying awareness and response in order to receive that funding. The District complies with that Act. ALL district workstations must be configured to be routed through the content filter server prior to going out to the Internet. Any special consideration for exemption of this policy will be for district employees whose workplace is outside of the District Wide Area Network (WAN). In such cases, a modem may be used for Internet access upon approval of the Director of Instructional Technology and the data Processing Manager. Standalone content filter software should be loaded on any computers outside the WAN accessing the Internet via a modem.

School volunteers with a need for Internet access must sign the Acceptable Use Policy for Volunteers. Administrators will complete an Active Directory Account Request form for school volunteers that have an established need for staff-level access. This form should be submitted to the Director of Inservice and Instructional Technology. (https://www.santarosa.k12.fl.us/pdc/docs/)

Internet Communications and Safety

The creation and/or use of Internet communication forums, such as blogs and wikis, must be limited to educational purposes and be in keeping with behaviors within the AUP and related guidelines. Student use of communication forums will be conducted under the guidance of a faculty member.

Internet Safety Awareness Campaign – The school district in partnership with the CEO Roundtable and the Sheriff's Office of Santa Rosa County, has adopted ~~the i-SAFE~~safety curriculum for teachers, parents and students. Awareness activities to promote internet safety throughout the district and community include: newsletters, marquee announcements, web resources, parent/teacher training, and media coverage.

During pre-planning, employees will be provided Internet safety and cyberbullying prevention training that will be documented at each site. Each site will develop an action plan to integrate Internet safety and cyberbullying prevention into the student instructional program.

Student Guidelines

1. The content filter will be configured to block all sites that are obscene, contain child pornography, are harmful to minors, or are determined to be inappropriate for minors.
2. Generally non-educationally-oriented e-commerce sites will be blocked for students by the content filter.
3. All chat rooms and other forms of direct electronic communications will be blocked.
4. Email will be screened for inappropriate words. Teachers are required to sponsor student email accounts (ePals, Gaggle.net, or if available, ~~I-mail~~district student email) on behalf of any student who needs this service. The sponsoring teacher has the primary responsibility to monitor these email accounts and ensure they are used appropriately. District personnel will~~The I-mail administrator at the PDC will~~ conduct random audits of district student e~~I-~~mail accounts.
5. "Hacking" and other unlawful activities online, and unauthorized disclosure, use and dissemination of personal identification information is prohibited.
6. Students at all grade levels will receive instruction on appropriate online behavior – including interacting with other individuals on social networking sites and in chat rooms – and cyberbullying awareness and response.

School board employees have the responsibility to notify the Content Filter administrator of any known sites that should be blocked. School Board employees may complete the form provided on the content filter page to request that a site be opened. Once this form is completed and submitted by the employee, the form is electronically sent to a committee comprised of representatives of Data Processing and Instructional Technology, including the manager/director of each. This review will be done in a timely manner and decisions made based on instructional quality, needs, inappropriate pictures or material, availability of chat and message boards, privacy policy, and availability of other alternative sites. The requesting employee will receive notification of the decision of the committee by the Content Filter administrator.

The District's Acceptable Use Policies (AUP) will be reviewed yearly by the District Technology Committee and approved by the School Board. Though there are acceptable and unacceptable uses of the Internet that are common for both students and staff, the District will use separate AUPs for students, volunteers, and employees. Parents and students 18 years and older must sign the Acceptable Use Policy Agreement for use of the Internet on a yearly basis. Employees will receive a copy of Acceptable Use Guidelines, annually. Questions regarding the guidelines should be directed to the Director of Inservice and Instructional Technology.

Copyright and Trademarks

Board policy requires that employees respect the Copyright Law and the right of copyright owners. Copyright law information has been provided to each school library media center for reference. An individual may be breaking the law if he/she reproduces or uses a work created by someone else without permission. Permission may be granted in the following ways:

1. Language contained within the work permits use of the material
2. Written permission has been obtained
3. Use falls under one of the special Fair Use privileges provided in the law

Whenever you are unsure about using a copyrights work, obtain permission from the copyright owner.

Posting or Transmitting Works

Reproducing or distributing copyrights material on the network or posting such material to a website is strictly prohibited, unless the material is in the public domain, is in accordance with the fair use provisions of the copyright law, or is distributed or posed with permission of the copyright holder. Use of copyrighted materials for distance learning is governed under an amendment to the law, the TEACH Act. (Please reference information in the media center.)

School Board Rights

Works created specifically for the use of a school or the school board, and/or to represent the school or school board, such as a school website, are the properties of the school board, even if created on the employee's time and with the use of their materials. (Also see Board Policy concerning copyright.)

Employee Rights

Employees own the copyright to works created outside of their employment responsibilities and without the use of school board resources. Employees may post such work on the school board or school website as long as notice of such posting and claim of ownership is provided to the webmaster of the site. By posting such work to the school board's or school's website, the employee grants a nonexclusive license or permission for any staff or student within the district to freely use such work.

Trademarks

Trademarks, such as logos and names representing a company, are protected under Trademark Law. Permission should be obtained prior to using trademarked names in any widespread publications, such as on the web.

Plagiarism

Plagiarism is defined as taking ideas or writings from another person and presenting them as if they were your own. Cutting and pasting others' materials into one's own document is considered plagiarism if appropriate credit to the original source is not given.

A charge of plagiarism may be avoided by:

1. Creating original materials, or
2. Giving credit to the source of the materials

Licensing

A license is a contract. In a school setting, it is most often associated with the use of networks, software, videos, and other audiovisual resources. The license governs the use of these materials. The user has no greater rights than those stated. Since each license is different, users should contact the individual in their school or district most familiar with the license agreement in order to comply with the requirements.

Licensing is required for transmitting any copyrighted materials over a network, whether it is a data network or closed circuit television (CCTV), especially if the CCTV network extends beyond one school. The following applications require licensing or written permission:

1. Computer software placed on a server or network for multiple-user access
2. Entertainment videos used for instructional or non-instructional purposes
3. Programs taped off-air under the 10-day use, 45-day erasure guidelines
4. Purchased or rental videos with the "Home Use Only" warning label
5. Instructional videos that require purchasing of closed circuit right or prohibit closed circuit use

Safety

Santa Rosa County School Board cares about the safety of all network users. Employees who receive, or become aware of others receiving, threatening or inappropriate communications should notify their supervisor, immediately.

Good online safety practices for employees and students include:

1. Not sharing personal or private information through email or the Internet
2. Not sharing financial information through email or the Internet
3. Ensuring students are aware of the Acceptable Use Policy and guidelines
4. Setting educationally relevant objectives for all student technology activities
5. Previewing Internet sites for educational value and appropriateness
6. Realizing that filtering isn't foolproof
7. Placing computers in central locations in the classroom or media center, where screens are highly visible

Security

Employees shall access electronic resources in a manner that does not compromise the security and integrity of these resources such as allowing intruders or viruses. Users wishing to download any document, file or software must observe district policies and procedures for virus checking and system security.

Users may occasionally be required to update registration, password, and account information in order to continue network access.

Privacy

Communication

The school board reserves the right to log, monitor, examine and evaluate all usage of its electronic resources, including email. Communications received or transmitted using electronic resources are not private despite any such designation by either the sender or the recipient.

The existence of passwords and "message delete" functions do not restrict or eliminate the school board's ability or right to access communications and information on electronic recourses. Messages sent over the Internet to recipients outside of the district should not be considered secure inside or outside of the network even if encrypted.

Confidentiality

Access to certain information and files is restricted to protect the administrative security of the school board and its records, and to protect rights relating to privacy and confidentiality. Employees who are provided access to such restricted information and files shall exercise the utmost care to prevent unauthorized persons from gaining access to them and to maintain the confidentiality of such information.

Users will take precautions to protect access to their accounts, ensuring that passwords are not accessible by others. The use must log out when leaving the computer workstation to ensure others do not use the account.

Confidentiality and Handheld Devices

Information from any school board data source(s) may not be downloaded into any handheld device without specific permission from the administrator responsible for that data.

To maximize the protection of student data on handheld devices:

1. Download only information that is critical to the job function
2. Ensure the device is password protected
3. Protect the device from damage, theft, or unauthorized use

Email Guidelines

Employees who access email accounts, either school board provided or private, via the district network must abide by the terms and conditions of the Acceptable Use Policy and related guidelines.

Subscriptions to Internet listserves and/or groups should be limited to professional or educational uses due to the amount of email traffic generated by general subscriptions.

Employee email addresses must be shared with interested parents and community members.

Parents and guardians must submit a written request for any non-public record information regarding their student that they wish to receive via email. Further, they must confirm their continued desire to receive said email communication prior to the sending of each such email. Schools are strongly encouraged to use other forms of communication when sending non-public information to parents/guardians; however, if the information is requested by a parent or guardian to be received via email, the school will use the following steps.

1. Parent/Guardian Request for Student Information via E-mail form is completed with parent/guardian during conference (or sent with parent/guardian for completion and subsequently returned to school).
2. Teacher maintains original and gives a copy of the signed form to site administrator.

3. Parent/Guardian emails teacher to request the information addressed in the initial form, as the information is desired.

In addition, security information such as username or password should not be sent via email for any reason.

Attachments to email messages should only include data files. At no time should program files (typically labeled ".exe") be attached due to software licensing requirements. In addition, there exists the real possibility that any program files received as attachments over the Internet may include viruses or other very destructive capabilities once they are "launched" or started. Messages with these attachments should be deleted immediately.

Email Retention and Archiving

Scope and Intent

This policy shall apply to all employees of the Santa Rosa County School Board in the conduct of their official duties.

The intent is to assist employees in using electronic messages while complying with Florida's Public Records Law, Chapter 119, Florida Statutes. It is not meant to limit or discourage the use of email for conducting business. Rather, it is to establish a framework for the proper use of email as an official business tool.

Public Records Law in Florida

Florida Statutes, Chapter 119 defines "public records" broadly as:

> "All documents, papers, letters, maps, books, tapes, photographs, films, sound recordings, data processing software or other material, regardless of physical form, or characteristics, or means of transmission, made or received pursuant to law or ordinance or in connection with the transaction of official business by any agency."

More narrowly, the Florida Supreme Court interprets this as applying to materials made or received by an agency in connection with official business that are used to perpetuate, communicate, or formalize knowledge. All materials of this type, regardless of form, must be saved and are open for public inspection, unless the legislature has specifically exempted them from disclosure. Exemptions include email containing student or employee health-related information.

How the Law Affects You as a Santa Rosa County School Board Employee

As indicated, email created or received in connection with official business that is to "perpetuate, communicate, or formalize knowledge" is subject to public records law. Such messages must be retained and are open for public inspection. However, not all official email is of this type. It is important for employees to know the distinction, so they can satisfy the relevant legal requirements in all cases.

If any of your email does fall within the public records category, you may not delete it, except as provided in the District's record retention schedule. Moreover, unless it is covered by one of the specific exemptions described below, it must be produced for any person upon request. A person need not state a "legitimate" need for public records to be entitled to inspect them. Persons

requesting email records must specify authors and dates. Student names should be eliminated prior to releasing the email to anyone other than immediate family members.

Transitory Messages

"Public records" are viewed as having enduring official significance and must be saved. On the other hand, most communications via email have limited or no enduring official significance. Recognizing this, the state's Office of the General Counsel and the Bureau of Archives & Records Management have defined a record series entitled "transitory messages."

Transitory messages are created primarily for informal and/or short-lived communication, as opposed to the perpetuation or formalization of knowledge. Transitory messages do not set policy, establish guidelines or procedures certify a transaction, serve as a receipt, or the like. The informal, time-limited nature of transitory messages can be compared to communications during a telephone conversation or in an office hallway. Transitory messages generally include, but are not limited to voice mail, self-sticking notes, and email messages with short-lived or no administrative value. Transitory messages may be deleted immediately following the related event.

Retention Periods for Official Records

Official records are those created or received in the course of official business, and they relate to official business. This is in contrast to purely personal records, which do not relate to official business. District policies regarding personal uses of district computers are presented elsewhere and are not covered by the policy outlined here.

Retention periods for official records, including those in email form, can be found in the District's general records schedule. This is available from the Finance Department. It incorporates items from the General Records Schedule for State & Local Government Records (GS1), the General Records Schedule (GS7) for Public School Records, and other Santa Rosa County School Board's retention schedules.

Retention schedules for official records are based on informational content, not format. In this context, most email messages fall into one of two categories:

1) *Public Records—*
Retain for Three Fiscal Years (please see note below).

These are messages that perpetuate, communicate, or formalize knowledge. Examples are general correspondence, inter-school memoranda, and most fiscal and budget documents.

2) *Other Records—*
Retain Until Obsolete, Superseded, or Administrative Value is Lost.

These are items that lose significance when they have served their purpose. This can be judged by the sender of the message(s). Examples include, but are not limited to:

- Transitory Messages, as defined above
- Routine announcements and information, including notices of meetings or workshops, queries regarding processes or ideas, and general information regarding programs
- Reference files that contain general information used in daily functions of the administrative area
- Meeting notices, statistical records, reading files, and inter-departmental memoranda

For category 1 (public records), administrative offices are required each year to file "records disposition requests" with the Bureau of Archives and Records Management for obsolete items that they wish to destroy.

For category 2 (other records), Florida Administrative Code, Rule 1B-24.010(3), allows state agencies to dispose of such items without having to fill out a records disposition request. For example, both duplicates and master copies of all transitory messages may be disposed of by a department when, in the judgment of the school or department, they are obsolete, superseded, or have lost their administrative value.

In particular, email items created or received that are of the "transitory" type may be deleted at the user's discretion, under the above standards. By contrast, email items of the "public records" type, such as official correspondence or sender's memoranda, must be kept through the three-year retention period, and they may not be deleted until records disposition requests have been submitted and approved.

Exemptions from Public Records Law

State and federal law exempts certain documents and information within documents from disclosure, no matter what their form. The exemptions that apply most often to Santa Rosa County School Board's records include:

1) Documents involving personnel matters that are confidential under Florida law (e.g., performance evaluations);
2) Student records that are confidential pursuant to the Buckley Amendment (e.g., course grades); and
3) Certain research records that are confidential under Florida law.

Before any email is released pursuant to a public records request, all exempt information in it must be deleted.

"Copy of Record"

By generally accepted practice, **the sender's copy** of a document is designated as the "copy of record." It is this copy to which the record retention requirements apply. All other copies are regarded as "duplicates," and they can be disposed of at will.

However, **this does not apply to email received from outside agencies or from the public**. All such received messages are regarded as copies of record, and if their content qualifies them as public records, they must be retained.

Handling Email Documents as Public Records

Florida's public records law offers a challenge to the use of email, because often email is exceptionally informal and efficient. By means of email, users find it easy to reduce or eliminate the normal handling, filing, and archiving tasks associated with hard copy. Consequently, they may not have any systems in place for periodically reviewing, storing, or deleting email.

Official email, whether "public" or "transitory," should be deleted only after it has been retained for the correct time period, as determined by the retention schedule. On the other hand, bear in mind that an official record that remains stored and accessible after the required time has elapsed is still an official record, and it must be produced upon request.

Given these facts, a systematic deletion program can be beneficial to both the employee and the institution—not only by eliminating obsolete and potentially misleading documents from the file, but also through saving resources, by not storing information unnecessarily beyond the appropriate time lines.

Methods used for reviewing, storing, or deleting email can vary according to individual choice and still be acceptable. In particular, as a Santa Rosa County School Board employee, you can comply with the retention requirements of public records law by one or both of the following means:

1) Printing your public record email and storing the hard copy in appropriate subject matter files, as you would any other hard-copy materials;
2) Electronically storing your public record email, using the means offered by our Outlook email system, such as archiving.
3) Every employee should create an archive file at the beginning of each school year, include the school year in the name, and save it into their personal "My Documents" folder or if applicable, the backup drive provided to staff at the site.

Printing email does enable you to keep all information on a particular subject in one central location, appropriate to its historical and archival value. If you choose this method, it will require not only that you print each public record message that you send, but also that you determine, having sent an email message, whether or not it must be saved under the public records law. You must also determine if incoming email must be printed, before it is deleted from your system.

Regardless of the method chosen, remember that ultimate responsibility for complying with the public records law is on you, the individual email user.

Responding to a Public Records Request

Public records requests may be made in writing or orally. All such requests should be referred to the appropriate school or departmental administrator. The administrator is responsible for appointing one or more persons to gather the requested documents, and then either arranging a time for inspection of the documents or making copies available to the requestor.

Email that does not fall within the definition of a public record should not be produced. Email that is a public record but contains exempt information should be produced, but the exempt information must first be deleted or redacted. If in doubt as to whether an email message is a public record or contains exempt information, the school or department administrator should contact the Finance Department.

If the person making the records request wishes to obtain copies of the documents, the public records law allows the District to charge 15 cents per one-sided copy. Also, if producing the public records requires extensive use of information technology resources or clerical and/or supervisory assistance, the District may assess a reasonable service charge, based on the District's actual incurred costs. An estimate of the charges should be given to the requestor and approval obtained prior to responding to the request. All charges should be collected before producing the documents.

Frequently Asked Questions

Q: What do I do when a reporter calls asking for my email?

Notify your school or department administrator, who will coordinate with the District office the gathering of the public record email documents that need to be given to the reporter.

Q: Does a requestor need to show a "legitimate interest" in my public records email before being allowed to see it?

No. Any person has the right to request to see a public record for any reason.

Q: Does a requestor have the right to conduct a "fishing expedition" and make "over-broad" requests?

Yes. The law does not require the requestor to specify a particular document. You should call your immediate district level supervisor when responding to "over-broad" requests to seek advice on whether the request can be narrowed.

Q: Can I recover the costs of producing public records documents?

Yes. If the labor or technical resources required to produce the requested public records are extensive, you can assess a reasonable service charge based on actual costs. You can also charge up to 15 cents per single-sided photocopy or laser printed page. You should provide the requestor with a cost estimate and collect all charges before producing the documents.

Q: May I refuse to respond to a public records request because I don't have the time to gather the documents?

No. However, if responding to a public records request requires a substantial amount of time, the law allows you to charge the requestor for the cost of that time.

Q: How do I determine what information is exempt from the public records law?

Contact your immediate district level supervisor and/or the District Finance Department.

Q: Am I required to produce personal, non-business-related email upon request?

No. Only email sent or received in connection with the transaction of official district business, as defined above, must be produced.

Q: How quickly must I respond to a public records request?

The law requires you to respond within a reasonable time, which will depend on the nature of the request. However, the courts have made it clear that public records requests are to be given a high priority.

Q: May I require requestors to put public records requests in writing?

No. Oral public records requests are as valid as written requests. However, you may ask for the request to be given in writing so there are no misunderstandings about what information is sought.

Q: Must I produce my public record email in a particular format?

No. You are required only to produce existing records. The law does not require you to create new records.

Q: Does the public records law require me to answer questions regarding the content of public record email?

No. You are required to produce the documents, not to explain them. You do not have to answer any questions, although at times it may helpful to do so.

Q: If the person who sent me a public record email asked me to keep it confidential, can I refuse to produce it?

No. If a document is a non-exempt public record, it must be produced upon request, even if the sender has asked that it be kept confidential.

Q: What happens if I refuse to turn over a public record upon request?

A person who knowingly violates the public records law is subject to disciplinary action and may be found guilty of a criminal law violation.

Q: If I keep district public records at a location other than my office, must I still produce them upon request?

Yes. All non-exempt public records must be produced, regardless of where they are physically located.

Q: What if the requested document contains exempt and public material? Can I withhold the entire document?

Not usually. When possible, the law requires you to delete the portion of the document that is exempt and provide the remainder of the document to the requestor.

Web Site Guidelines

General Introduction

The School Board of Santa Rosa County maintains a range of websites accessed through its primary site at https://www.santarosa.k12.fl.us/. These sites allow communication between the district, employees, students and the community. The district, school, and teacher web pages that comprise the School Board of Santa Rosa County websites may be used for the sharing of school and district-related information, publishing district policies, and the delivery of curriculum and instruction. All electronically-delivered materials must be consistent with the educational goals of the School Board of Santa Rosa County.

All official websites and/or pages that represent a school, school-based organization, department, or other Santa Rosa County School Board entity must follow the school board's Website Guidelines. Official websites or pages are defined as those that have been approved as to format

and content by a school's principal or administrator designee or, in the case of district/ departmental websites or pages, by the department administrator or his designee and are monitored for compliance.

Hosting of Websites

All official sites representing the district will be hosted on servers located within the network of the School Board of Santa Rosa County or on approved alternate host sites. Teacher/staff pages – including communication tools such as, but not limited to, blogs and message boards – will be considered official sites and must also be hosted on district servers, on-site at the school or on a site approved by the Director of Inservice and Instructional Technology or the District Technology Committee (see Approved Alternate Web Host List at https://www.santarosa.k12.fl.us/pdc/docs/).

Official sites representing the School Board of Santa Rosa County will be hosted in one of the following ways:

1. School and Classroom sites
   a. District web server for schools
   b. District solutions such as Santa Rosa Moodle or SharePoint
   c. District-Approved Alternate Web Hosting sites
2. Student sites
   a. Intranet
   b. Classroom website (teacher-managed/student work posted by teacher)

Publishing Requirements:

A. School administrators are responsible for school web site content and will monitor their school webs, regularly.

B. Each school will identify a webmaster who is a district employee.

C. The homepage of each website will include a return link to the School Board of Santa Rosa County homepage https://www.santarosa.k12.fl.us/.

D. The homepage of each website will include an email link to the school webmaster.

E. Each website must comply with district policy on the posting of student images, names, and/or student information as per Board Policy.

F. The posting of copyrighted material must comply with the Copyright Law and follow the guidelines in the Copyright and Trademarks section of this Employee AUP and Implementation Guidelines document.

G. Website developers must make every effort to comply with Section 508 (Level 1) of the Rehabilitation Act Amendments requirements.

H. Website developers must take extra precautions to ensure compliance with the privacy laws set forth in HIPAA and FERPA.

I. A custom domain name must be owned and maintained by the school if it is to be used as an official website address for the school.

J. Web sites, including teacher sites on Approved Alternate Web Hosts, should be edited and updated on a regular basis by the individual responsible for that web and must be free of any spelling or grammatical errors.

K. Linking from an official school/district site to other websites that are not approved as official is only permitted when a disclaimer (see below) appears at the point of the link on the official site and on those sites being linked stating that these are not approved sites and neither the format or content has been approved, endorsed or sponsored by the School Board of Santa Rosa County or the school.

The following wording will be used for the disclaimer. [Neither the School Board of Santa Rosa County, Florida nor any of its schools approves, endorsed, or sponsors the format and content of this site.]

A linked site that does not follow the School Board of Santa Rosa County's Acceptable Use Policy and Implementation Guidelines is not considered official.

The following district policy guidelines also apply to all student work published on the web:

- Published documents may not include a child's phone number, street address or box number, or names of other family members;
- Publish student name, photo, and creative work only with parental permission (cf. Acceptable Use Policy for Students);
- Documents may not include any information which indicates the physical location of a student at a precise time other than attendance at a particular school or participation in school activities;
- Documents may not contain objectionable material or point to objectionable material as stated in the Santa Rosa County Acceptable Use Policies;
- Students must not work directly on teacher, school, or district department websites without express, written permission from the district Web Administrator and Director for Instructional Technology.
- Students must not create or work directly on "live" school club/organization websites (e.g., robotics team websites) or any website that represents the district. Students should work on local copies of these websites, which can then be published on a district-approved Web server by an appropriate staff member.
- Students must not construct websites using content or links that violate state or federal laws.

DO

The following are expected behaviors:

- Use a consistent design with clear navigation throughout the website.
- Reduce impact on bandwidth by:
    - Keeping the graphics, sounds and animation to a minimum
    - Minimizing the use of multimedia such as Flash and providing a text bailout link
    - Avoiding the use of large images. Control image size by using image-editing software, not HTML. Use thumbnails when possible.

- Keep the length of a page manageable. Use anchors (targets or bookmarks) to allow quick access to sections of long pages.
- Assign ALT text to images to provide access to the sight-impaired.
- Keep links current.

DON'T

The following activities are not permitted:

- Using slang or objectionable language
- Posting pages under construction
- Posting commercial information. Sponsorships and business partnerships may be appropriately acknowledged on district-supported pages.
- Allowing students to participate in online forums or chat areas that are not moderated by an instructor in a classroom setting
- Using web pages or web forums to solicit personal information from students

Consequences/Due Process

Standards of Conduct

Standards of conduct are necessary to assure that people expressing their own individual rights do not violate the rights of others.

a. Employees misuse of the system is defined in the Acceptable Use Policy and related guidelines. The definitions stated are not exclusive. If an employee is capable of inventing a new way to misuse the system, and it is reasonable that the employee would know these actions are improper, the employee may be disciplined.
b. Employees should report system abuse to their immediate supervisor for appropriate action.
c. Employee use of electronic resources is a privilege granted as a result of the employee's work status and is not a legal right. The school board may restrict any employee's use if the privilege is abused.
d. If an employee uses an electronic device to gain prohibited access to an account that the school board has through a lease, rental agreement, or other contract with a third party, the employee will be subject to disciplinary action. This may include the notification of the appropriate state or federal law enforcement agency.

Consequences

If an employee violates any of the preceding policy provisions, his/her access may be limited or terminated and future access may be denied. In addition, appropriate disciplinary actions may be taken which may include, but are not limited to, a letter of concern, suspension with or without pay, termination, legal action and/or referral to law enforcement as appropriate.

Warranty

The school board makes no warranties of any kind, whether expressed or implied, for the communication/data/networking services it is providing. The school board will not be responsible for any damages a user suffers. This includes loss of data resulting from delays, non-deliveries, miss-deliveries, or service interruptions caused by the school board or as a result of the school board's negligence or by the user's errors or omissions.

Use of any information obtained via the Internet is at the user's own risk. The school board specifically denies any responsibility for the accuracy or quality of the information obtained through its services. All users need to consider the source of any information they obtain and consider how valid that information may be.

The school board will not be responsible for any financial obligation arising through the unauthorized use of the school board's electronic resources.

Opinions, advice, services and all other information expressed by system users, information providers, service providers, or other third party individual sin the system are those of the providers and not necessarily the school board.

The Santa Rosa County School Board will cooperate fully with local, state, or federal officials in any investigation concerning or related to misuse of electronic resources.

Carefully read the Acceptable Use Policy for Electronic Resources and Implementation Guidelines.

Inappropriate use of electronic resources may be grounds for disciplinary and/or appropriate legal action, including termination.

As reminder of appropriate use, a warning screen will appear on the user's computer at logon and/or other times.

Forms

Most documents mentioned in this policy can be found on the district documents and forms web page at http://www.santarosa.k12.fl.us/pdc/docs/, are in Microsoft Word (DOC) or Portable Document Format (PDF) and are available for download at the website locations indicated.

Public Hearing Approved and Advertised: July 26, 2012

Public Hearing Held: Sept.6, 2012

School Board Approved and Adopted: Sept.6, 2012

School Board Approved Revisions: _____