Tim Forson
Superintendent of Schools

40 Orange Street
St. Augustine, Florida 32084
(904) 547-7500
www.stjohns.k12.fl.us

MANAGEMENT DIRECTIVE 5.01

Revision 14

DATE: May 26, 2017

TO: All Employees

FROM: Tim Forson, Superintendent

SUBJECT: Acceptable Use Procedures and Guidelines

REF: School Board Rule 6.83, Acceptable Use Policy (AUP)

Introduction

School Board Rule 6.83 contains the District's Acceptable Use Policy (AUP). This document provides supplemental Acceptable Use Procedures and Guidelines for employees. The AUP along with these procedures and guidelines ensure the safety, reliability, accountability, network and data integrity and security of the digital network and other district technology resources. It also protects our students, staff and technology resources.

Guidelines for Employees of St. Johns County School District Network and Technology Resources

1. Acceptable Use of the Digital Network of the St. Johns County School District

- Employees' use of the District's digital network, internet service and other electronic resources is a privilege. As a condition of that privilege, employees must comply with this Acceptable Use Policy ("AUP"). The following general rules govern employees' use of the District's digital network and technology resources:
- The use must be in support with the District's educational goals and policies.

- The use must comply with the Acceptable Use Policy ("AUP"), Board Rule 6.83 and these procedures and guidelines.
- The use must comport with the six pillars of CHARACTER COUNTS!
- Requires that employees who access our network with district or personally owned electronic equipment ANNUALLY sign this Acceptable Use Agreement, which is to be kept on file at each school or district department.
- The use must comply with applicable laws and regulations, including bullying and harassment.

2. Prohibited Activities

The following are prohibited activities:

- Attempting to access, modify, harm or destroy another user's data on the network.
- Attempting to subvert, defeat or disable installed web or network access filters, workstation security software, antivirus software or other features, network firewalls or other measures in place to secure the school district's technology resources.
- Use of remote access software or services to access remote computer networks, workstations or servers from the district system.
- Attempting to interfere with the normal operation of computers, terminals, peripherals, or networks.
- Usage that may invade the privacy of others.
- Experimentation with software or hardware using district resources.
- Changing, deleting or modifying Internet browser settings including hiding or deleting Internet history or records of Internet use.
- Any use constituting a crime or violates any state or federal laws.
- Any use that would make the user or the School District liable in a civil action, or that could adversely affect the School District's eligibility for any grant, certificate, status, waiver, or benefit.
- Any fraudulent or deceptive use.
- Use of file sharing software and or services to access or share files, folders or other digital information.
- Publishing, altering or deleting code, content, or data without appropriate authorization.
- Use of Internet conference or web video conferencing software or services that transmit unauthorized student images, video or other identifiable information to remote users.
- Setting up, configuring or maintaining private servers within the District without explicit written permission from the SJCSD Information Technology Department.
- Violating terms of applicable software purchase, licensing, or acquisition agreements or infringing any patent, copyright, trademark, or other intellectual property right.
- Any use specifically prohibited by the Chief Information Officer or his or her designee after written warning.
- Assigning students to perform any kind of repair, installation or support for District technology equipment.

3. Enforcement

Employees who violate these procedures may be denied access to St. Johns County School District computing or technology resources and may be subject to other penalties and disciplinary action, including dismissal.

AUP violations will be tracked by schools and departments to prevent future occurrences.

4. No Expectation of Privacy

Employees have no expectation of privacy in their use of the District system.

5. Public Records

Employees using the St. Johns County School District's Digital Network (and other resources) recognize that they are bound by State Public Records Laws (Chapter 119, Florida Statutes). Documents that are created to formalize knowledge or transact school or district department business are considered public records open to the review and copying of the general public. This includes all work records on individual computer systems, e-mail, and data transmitted over the server from on-site or off-site locations, and portable media such as disks, floppy disks, flash drives, CDs or any other transportable media. All records must be retained according to the Department of State, General Records Schedules (GS1-SL and GS7) and in accordance with Chapter 119 of the Florida Public Records Statute. See the St. Johns County School District website for links to these documents.

6. E-mail

For purposes of this document, e-mail includes point-to-point messages, postings to newsgroups and any electronic messaging involving computers and computer networks. Organizational e-mail accounts, including those used by student organizations, are held to the same standards as those for individual use by members of the St. Johns County School District of Florida community. E-mail is also generally subject to the Florida Public Records Law to the same extent as it would be on paper communication. St. Johns County School District hosted and supported email accounts are made available to school district employees, approved contractors and approved charter or contract school administrators. Any email account or software which is not considered standard will not be supported or maintained by school district technology staff or resources.

A. Employee Responsibilities

- Your St. Johns County School District e-mail account is for your use only. You are responsible for all activities that originate from your account.
- You are responsible for the security of your password. You should choose passwords that cannot be easily guessed. Passwords must be safe guarded and not shared with others.
- You are responsible for understanding, following, and keeping up to date with St. Johns County School District e-mail service procedures.
- You must comply with all local, state, and federal laws, and St. Johns County School District policies or procedures.
- You must use your correct name and computer account in all electronic mail and messages.
- You are responsible for protecting your files from reading or writing from unauthorized users.
- Users must comply with public record retention laws when deleting e-mail.
- Users are responsible to avoid vulgar or inappropriate language when using e-mail.
- Users may be held liable for deleting computer data that is subject to legal prosecution or spoliation claims (the act of destroying evidence in advance or during litigation).
- Staff should to the maximum extent possible avoid emailing any student Personally Identifiable Information (PII) data that includes ESE disabilities, State test scores, discipline details, report cards, and other specific academic record details.

B. Use of District E-mail

While not an exhaustive list, the following uses of e-mail by individuals or organizations are considered inappropriate and unacceptable at the St. Johns County School District. In general, e-mail **shall not** be used for the initiation or re-transmission of:

- Chain mail that misuses or disrupts resources - e-mail sent repeatedly from user to user, with requests to send to others.
- Harassing or hate-mail - Any threatening or abusive e-mail sent to individuals or organizations that violate St. Johns County School District rules and regulations.
- Virus hoaxes.
- Spamming or e-mail bombing attacks - Intentional e-mail transmissions that disrupt normal e-mail service.
- Junk mail - Unsolicited e-mail that is not related to St. Johns County School District business and is sent without a reasonable expectation that the recipient would welcome receiving it.
- False identification - Any actions that defraud another or misrepresent or fail to accurately identify the sender.
- Transmission of unprotected student data including information that specifies any student name(s), number(s), and/or student academic record data.
- Personal business or personal communications that are not work related.
- Staff or Student SSN's, Credit Card numbers, Bank Acct numbers and network Passwords (unless encrypted as an attachment using 256 bit AES).

7. Anonymous E-mail, Chat Rooms Discussions, or Bulletin Boards

Users of the digital network are not allowed to send or forward anonymous or pseudonymous e-mail through an e-mailer or other software or decoding devices.

8. Copyright Infringement

Users of the digital network must comply with all state and federal copyright laws. For questions, users can contact the Media Services or Information Technology Department if there is any uncertainty whether an article or software is copyrighted.

9. Trademark Infringement

No symbol, logo, phrase, or other trademark from a document, website, or other source may be uploaded, downloaded, linked, or in any way transmitted without the express permission of the trademark owner.

10. Passwords

Passwords are for internal use and are to be kept confidential. Employee user account passwords shall not be shared with or disclosed to students, interns, other employees, visitors or friends. Passwords are tracked for accountability and security to a specific user.

11. Off Site Use of District Computers

Users shall have no expectation of privacy when conducting school business at off-site locations using district owned computers and other mobile technology. Additionally, users must adhere to all the same procedure restrictions as if they were using the computer at the school site when conducting school business.

12. Litigation

In the event of litigation, all computer users are on notice that federal and state civil rules of procedure may allow discovery of all computer hardware and software. This includes, but is not limited to, computers, laptops, home computers, printers, cell phones, and other electronic equipment that is used to conduct school business. Any attempt to damage or destroy evidence may trigger civil and criminal penalties (known as spoliation claims). If users' equipment is subpoenaed or litigation is anticipated, contact the Human Resources Department for guidance on how to proceed.

13. Support of District Owned Technology Devices and Network Infrastructure Equipment and Software

Employees assigned to the District IT Department are the only individuals authorized to implement, configure, support, modify or create any network infrastructure equipment or software. This includes, but is not limited to, basic network devices such as hubs, switches, routers, network firewalls, and wireless access points. Wireless access points must be authorized by the Information Technology Department.

Employees assigned to the District IT Department are the only individuals authorized to repair or modify district owned technology resources. All requests for repair or service shall be submitted via the District's web based ticket system. Unauthorized employees who damage a system due to improper or unauthorized repair or other misuse may be held liable for the repair or replacement costs where applicable.

Schools and departments are prohibited from designating, sponsoring or assigning students or interns to perform any kind of maintenance, repair, configuration or installation services to support District owned technology devices or Network equipment. These tasks are performed by IT Department staff only.

14. The Use and Operation of Personally Owned Technology Devices or Electronic Property at School or District offices

Employees who are authorized to use or operate personally owned devices must adhere to the following:

- Any computer that is connected to the District Digital Network via wired or wireless control must have approved and functioning anti-virus software running with up-to-date virus definitions. Acceptable anti-virus software includes those by Norton/Symantec, McAfee, and Trend Micro.
- An Acceptable Use Agreement form must be signed and approved by the school or district department administrator prior to operating any personal electronic property in St. Johns County School District schools or offices.
- St Johns County School District employees are not authorized to perform any repair, configuration or maintenance on personally owned technology resources, that are brought to school property or present during school sponsored activities including both software and hardware resources.
- District employees are also not authorized to install any software on technology devices owned by other individuals. Any student, teacher, administrator or visitor who wishes to bring and/or operate their personally owned technology devices must apply and obtain permission from the local school or department via the *Waiver for Personal Electronic Property* form contained in this Acceptable Use Procedure.

- Schools and departments are prohibited from designating, sponsoring or assigning students to perform any kind of maintenance, repair, configuration or installation services to support personally owned technology devices that are brought to school property or present during school sponsored activities.
- Employees who are authorized to bring and/or use a personally owned technology devices are responsible for the safe keeping and proper use of their property. St Johns County School District is in no way liable for any loss or damage for personally owned devices.
- Schools/Departments shall not make provisions to hold or store personally owned devices.

15. Additional Requirements for Employees in the use and care of District Technology equipment

Employees are required to comply with the following:

- Teachers and administrators shall utilize their standard computer system that meets the administrative standard (outlined in the District Technology Plan) or was provided under the Technology Refresh Plan to access all district applications and network resources.
- Under the District Technology Plan teachers and key school administrators are provided a dedicated computer system that meets district standards for access and performance. These systems are to be used solely by teachers/administrators for security reasons.
- Teachers and administrators are responsible for the safe keeping of all digital content (data security) and appropriate use of the system at all times. Classified or sensitive information should be deleted when no longer needed.
- Employees are responsible to comply with all Security Awareness notes and procedures published. All Security Awareness notes/procedures can be found on the Intranet under the IT Department (https://inside.stjohns.k12.fl.us/security).
- Employees who are assigned district or school owned technology devices (i.e., notebook computer, cell phone, PDA, etc.) are responsible for the protection and safe keeping of these devices. Employees will be liable for any costs needed to repair or replace any assigned device that is lost, stolen or damaged due to negligence. Each incident will be reviewed by the Director of Purchasing on a case-by-case basis to determine liability.
- Employees shall sign and acknowledge the Employee Technology Equipment Responsibility form before equipment is assigned.
- Employees are not authorized to release, access, share or email protected student record data to school or classroom volunteers.
- School or district administrators who are authorized (by the principal or district department director/executive director) to electronically send or transmit sensitive or protected staff or student data must do so using approved and secure methods. The simple use of email (including district email) to send or receive protected student/staff data is not considered secure. For any questions, please contact the IT Department for more information on handling sensitive or protected student or staff data.
- Employees should avoid using district resources (primarily computers) to access, use or view personal email or webmail. Only limited use in extreme cases is authorized during non-duty times when approved by the supervisor. Employees should not setup personal webmail as their primary Internet screens (home screens) or configure auto logins to personal email accounts using district equipment.

16. Additional Requirements for Employees in the use of Video, Photo and/or Audio recording devices

This section covers the use of any device that can record audio, photo or video content in the school environment, particularly the classroom. Such devices include:

- Smart Pen (i.e. Livescribe Echo), Personal audio recorder
- Mobile/Smart Phone (i.e. iPhone), Personal Media Player/MP3/MiniDisc Player (i.e. iPod)
- Mobile Tablet or Slate Device (i.e. iPad, Nexus), eReader (i.e. Nook, Kindle)
- Mobile Computer System capable of recording video, photo, audio (i.e. notebook, netbook)
- Digital or film-based Camera or video recorder
- Digital or film-based Audio Recorder (i.e. Cassette player)

All employees must adhere to the following:

- Employees may possess instructional technology devices that record audio and/or video content and utilize them as instructional tools in the classroom only with the consent and under the direction of the school administration, as it pertains to the current curricular unit, lesson, etc.
- Except for open houses and public events as discussed below, no other videotaping or recording is allowed on school premises.
- No hidden recording devices are permitted.
- All recording capable devices must be turned off when not being used for an authorized purpose.
- Publication of recorded content (audio, video, and photo) without prior written consent from the principal is prohibited.

Open House and Public Events Exception.

Open house and public events are events where school premises are opened to the public or a segment of the public at the direction of the principal. They include: open houses, sporting events, plays, musicals, contests, fairs, fund raisers, awards/recognitions and theatre performances. They also include off campus events such as graduations, contests, fund raisers and other school sponsored public events.

In the exercise of judgment and discretion, a principal may also allow videotaping or photographing under other circumstances, provided that appropriate steps are taken to prevent unwarranted disclosure of student images contrary to their directory information opt-out election and to avoid disruption of the educational environment.

17. Teacher or school staff requirements regarding student Internet use

Teachers and other assigned staff who are charged with teaching or supervising children at school when using district computers to access the Internet shall comply with the following procedures:

- When inappropriate Internet use (or any other AUP violation) is discovered, the teacher or staff member shall (1) remove the student from the computer, (2) shut the computer down normally, (3) contact your school administration (4) school administration will contact the IT Dept, (5) take that computer out of use, or remove it from circulation altogether until the IT Dept can complete an investigation. The school level Technical Support Specialist (TSS) should assist the IT Dept staff (if needed).

- Teachers or school staff should monitor computer use in labs, classrooms and media centers to ensure students are using the Internet or other district applications for class or school related work. Teachers or staff shall actively monitor (barring ADA limitations) all student computer use in regular intervals not to exceed 10 minutes. Monitoring by teachers/staff to ensure students are using computers appropriately can certainly be more frequent. If monitoring software is being used, similar monitoring schedules or frequency should be followed. If classroom teachers can see students when they are actively engaged using computers (and the Internet) similar monitoring may be accomplished with little classroom roaming. Teachers can view a student's Internet history if there is a question about their previous Internet activity.

- Students shall receive a digital citizenship introduction each year before using school computers. Throughout the year, each student will receive lessons appropriate for the intended grade level in the following themes: Digital Etiquette, Online Safety, Plagiarism and Copyright, Cyberbullying, Security and Viruses, Information Privacy, Online Commenting, Evaluating Online Sources, and Effective Internet Searches. Additionally, teachers should strive to continually promote ethical technology behavior throughout content lessons during the school year. Teachers are responsible for ensuring that students are familiar with the AUP and understand the consequences of violating the AUP. Students will be responsible for appropriate choices.

- Teachers or staff should be looking for signs that students are hitting Internet filters. Students should be warned that hitting the Internet filter (and viewing the filter message and hearing the warning sound) is usually a sign of looking for the wrong Internet content.

- Schools shall track student computer use in the Media Centers and labs in at least one of three methods:

    - Institute a bar-coded checkout card for using each computer in the media center (if student Active Directory student accounts are not available).
    - Utilize individual student Active Directory user accounts if available (student login accounts are expected to be piloted at selected schools in the future).
    - Use computer monitoring software (like LANSchool).

- Students will not be allowed to use school computers without a current and signed Acceptable Use Agreement form.

Web Pages, Websites and Internet Guidelines

Administrator/Webmaster

The District Webmaster is responsible for maintaining the official St. Johns County School District web site that presents information about the school district. The District supports a consolidated website for district departments. All schools will use the district's content management systems and web servers to host their websites.

All official St. Johns County School District websites (which includes all school, teacher, or classroom web pages for educational purposes) must be hosted on district owned and operated computer server(s) on school district property and must adhere to procedures and guidelines of the Acceptable Use Procedures for the St. Johns County School District Digital Network. The District may authorize the use of websites not hosted locally but managed by the District. A list of approved supplemental websites which may be used to post school, teacher or classroom related content are available on the IT Department's section of our internal website.

External websites, websites not hosted or maintained by the school district, that are linked from school or district websites must adhere to the requirements outlined in Sections 6 and 7 below. The goal for our official district website is to provide a safe web-based communication tool to inform parents, students, district staff and the community about our district office, schools, programs and events.

Rationale

School web pages are public documents welcoming the outside world to the school and linking students and staff to outside sources of information. Guidelines are required in the construction of school web pages to ensure that information on the pages is appropriate for any Internet user to access and is free from content which may not be appropriate for students. Web pages must support the educational mission, goals, and objectives of the St. Johns County School District.

In producing informational/educational web pages, the following goals will be considered:

- Introducing outside visitors to the school and its programs.
- Sharing the school's successes with the world.
- Linking students and staff to good outside information resources.

Requirements

1. School Webmaster

Any school setting up a website must have a school webmaster appointed by the principal. The school webmaster will assist the principal in ensuring that guidelines are followed and that the content of the school web pages meets with the principal's approval. The school principal is the final authority with regard to school web pages.

Schools are required to publish and update common school information on their website which includes at a minimum: general information about school programs, athletics contact information (names, email address, phone numbers, roles, etc.), instructions, policies, rules, forms, schedules and events.

2. Content of Web Pages

Web page content may consist of text, images, links, documents, videos, audio files and presentations. All content of school web pages must be consistent with the educational mission, goals, strategic plan and objectives of the St. Johns County School District and School Board Rules. Content placed on web pages is expected to be grammatically correct and accurate.

The St. Johns County School District Information Technology Department reserves the right to immediately stop access to or from any site which may be in violation of this AUP or otherwise poses a risk to the district network, personnel or other technology resources.

3. Advertisements

School web pages may contain only small acknowledgments of school partnerships or sponsorships in the form of text, links, and images no larger than 300 pixels in height or width. School and District web pages may also contain links to District approved fundraising websites. A list of approved fundraising websites is available in the IT Department's section of our internal website.

4. Publishing Student Information Including Photos and Videos on School or District Websites

All District staff must use caution when publishing student information, photos of students, and/or content created by students (photos, drawings, written work, audio or video files) on their websites.

The following procedures apply:

- No web page content shall allow people accessing the web page enough information to contact any student directly or locate by providing a student's phone number, email address, location or any other private (non-directory) student information.

- Photos of students, videos of students, and students' full names may only be published online with permission from parents or guardians. This permission is normally granted by parents / guardians on the ***Release of Student Directory Information Options Form***, found in the Student Code of Conduct. Parents or guardians may opt-out of having their child's name or image published at any time during the school year. Before publishing any content which includes students, please check with your school's registrar to ensure that the proper permission has been granted.

- As a precaution, teachers should avoid identifying students by using students' first names, initials, or other codes, or listing the teacher's name and a number for each student, within the web page and with all file names.

5. Publishing Student Information Including Photos and Videos to External Websites

External websites are websites not hosted or maintained by the school district. Public web pages and any other form of electronic data transferred outside of the district's digital network must not contain any private (non-directory) student information. Schools should proceed with caution and sensitivity in this area. If teachers or staff publish student photos or videos to external websites, they must obtain the student's parent or guardian written approval prior to posting or publishing. It is recommended that parents or guardians be given an approval form to sign which explains the planned usage of the student information.

Schools who wish to fundraise by publishing digital photos or videos to external commercial websites for sale must comply with the following procedures:

- All receipts received shall be accounted for in the school's Internal Accounts.
- All transactions must be documented in each school's internal accounts.
- Schools may provide direct links to booster clubs or other organizations that exist solely to support the school, provided they comply with the procedures outlined in section 6 below.

6. Links to Websites Managed by Outside Support Organizations

This section pertains to external websites that are managed by clubs or organizations that exist solely to support the school (like a booster club). Schools may provide links on their official school websites to these external websites that provide a benefit and promote the school/district mission.

All external websites run by booster clubs and similar organizations which are linked from a school or district website must comply with the following procedures:

- They shall clearly show that they are not the official school site and are not in any way being updated or maintained by the school or district staff.
- They shall not display the school's address or imply that they represent the school or school board.
- They shall exist solely to support the school.
- They shall post clear disclaimers that they are not official websites of the school.
- They shall not contain any inappropriate content.
- They shall not link to any other websites that contain inappropriate content.
- School websites shall prompt the user when linking to external sites that they are leaving the official school/district website.

7. Links to Other Websites

This section pertains to external websites that are purely educational in nature. Schools may provide links to purely educational websites that provide a benefit and promote the school/district mission.

School or district websites linking to educational websites shall comply with the following procedures:

- External sites shall be purely educational in nature.
- External sites shall not contain any inappropriate content.
- External sites shall not link to any other websites that contain inappropriate content.

8. School Web Pages Requirements

All school web pages will conform to district guidelines and will contain:

- The name, address, and main telephone number of the school.
- A link to return to the school website's home page.
- A link to contact the school webmaster and/or principal.
- A link to the District website.
- A layout that is consistent with all other school websites.
- The name of the school inside the <TITLE> tag.

These items will be managed by the District webmaster. They will be automatically added to all web pages created with the district's content management system, so individual teachers and staff will not need to add them to their web pages.

9. School Web Page Recommendations

The following items are recommended:

- Avoid "Under Construction" or "Coming Soon" notices on web pages; construct the page before placing it on the web. If such notices are necessary, do not keep them on any page longer than four (4) weeks.
- The date of the last update to a web page or file should be included on information that is time-sensitive.
- Images should be displayed with width and height set. Images with a large file size exceeding 1 megabyte should be avoided. Include a brief description of the image in the <ALT> tag.
- Pages should accommodate a variety of popular web browsers, including text-only browsers.
- Documents created in Microsoft Word, Excel, Publisher or other word processing programs should be posted as PDF (Portable Document Format) files whenever possible.
- Avoid adding content or files that require unusual plug-ins or uncommon software to be viewed. If such content is necessary, include a link to download or install the required plug-in or software.
- Pages must be proofread for spelling, grammar and content accuracy before they are displayed.
- Periodically check the links on your web pages to ensure that they do lead to their intended location.
- Periodically review the content on your web pages to ensure that it is current.
- Facilitate navigation between each of your web pages, preferably in a navigation column on your web page.
- Keep URLs as simple as possible by giving files and folders succinct names and avoiding the use spaces and special characters in those names.

- All webmasters, teachers, and staff who create and edit web pages should retain backup copies of their web pages.

10. Web Content Developed by Employees

Classroom or teacher web pages, defined as pages that contain information about curriculum, class activities, homework, or other information directly related to education, are encouraged and must comply with the Acceptable Use Procedures. Each school's webmaster is responsible for reviewing classroom and teacher websites to ensure that they are in compliance.

Personal web pages, however, defined as pages that contain personal information about a district employee, their family, and/or their interests not related to school, are NOT permitted on district or school servers. Standards of conduct, including the use of social networking websites, blog websites, personal websites and other means of public broadcasting by employees is discussed in board rule 6.84.

11. Web Content Developed by Students

As part of class/course projects, students may be developing and publishing content on web page(s) for the Internet. When directing students to publish content on the Internet, please refer to Sections 4 and 5 of this document to ensure that student information is protected.

The following procedures apply:

- Students may create content for web pages, under their instructor's supervision, pertaining to classroom assignments, school events, or other activities.
- Students who create blog entries, podcasts or videos must comply with this AUP, follow the direction and supervision of their instructor.
- Blogs in use by St. Johns County School District students must be registered with their local school or department and must have a designated teacher who is responsible for approving and/or publishing all content posted to the blog.
- Students are not authorized to share or post personal photos and other profile information to public or school district websites when using district or personally owned electronic devices on school property or during any school sponsored activities.
- The St. Johns County School District Information Technology Department does not warrant nor guarantee access or data integrity of student developed web content. Any and all web content created for class projects or course work should be backed up frequently using local resources.

12. Web Content Developed by School Volunteers

Volunteers may be provided with remote accounts to access the District's content management system in order to create and update specific school web pages that reside on district servers. This will allow staff and/or volunteers to work closely or independently with school administrators to create, update and maintain school web pages that support various school programs, including athletics. It will also allow the school to better control and support all of its website content.

Schools that exercise this option must comply with the following procedures:

- All volunteer access must be approved by the school principal before a request is submitted.
- School volunteers will sign, understand and follow the District's Acceptable Use Procedures (AUP). All AUP forms are to be kept at each school or department.
- Schools must follow contractor account request procedures to request editing access for the school volunteer. Volunteers can receive training on how to access and use the school website so they can create, update and maintain specific school web pages.
- The school webmaster is responsible for all content posted by volunteers. The school webmaster will have access to edit or remove any content posted by the volunteers.
- If an AUP violation does occur by a volunteer, the school or district department webmaster shall immediately notify the District Webmaster. The School and District Webmasters will work with the volunteer to resolve the AUP issue(s).
- The District Webmaster will be responsible to revoke any volunteer account when notified by any school or district department or if the AUP is not followed.

Employee Acceptable Use Procedures Agreement Form and Bring Your Own Device (BYOD) Form

(Applies to employees who wish to use the District's digital network)
(**Optional**: Applies to employees who wish to use their own personal electronic devices in schools/offices)

Employee ***(Applies to Employees)***

I have read and agree to follow the St. Johns County School District's Acceptable Use Policy (Rule 6.83) and the supplemental procedures contained herein (Management Directive 5.01).

Employee Name: _____ (please print)

Employee ID Number: _____ (6 digit, network login ID Number)

School or Dept Affiliation: _____ (School/Dept)

Employee Signature: _____ Date:_____

School/Dept Administrator's Approval (School/Dept Designee)

The Supervisor verifies the employee and approves their access to the St. Johns County School District Digital Network. Approval is also granted to use a personal electronic device, noted below (if applicable).

School Administrator's name/position: _____ (please print)

Administrator's signature: _____ Date: _____

(Optional) Employee Bring Your Own Device (BYOD)
(Required for employees to operate personally owned technology devices in Schools/Dept's)

As an employee, I wish to bring my personal electronic device(s) to School or on District premises. I understand that responsibility for the care and use of this device belongs solely to me.

Requested Device(s): _____ (If applicable)

(Computer or mobile device make/model that can access the District network) (Excludes: Smartphones/cell phones)

Employee Technology Device Responsibility Form (2017-2018)

The District provides teachers and eligible staff mobile technology devices. The District is proud to offer employees an optional device insurance for eligible District owned mobile devices. Please complete the following information below to confirm your election options.
I have read and agree to adhere to all District Procedures/rules, including:
(**Please initial each**)

a) _____ Employee Acceptable Use Procedures (AUP)
(Management Directive 5.01 and School Board Rule 6.83)

And

b) _____ Employee Technology Device Terms and Conditions Document, including all program insurance information

And

c) _____ I (**Elect** or **Decline**) (*circle option desired*) to participate in the optional SJCSD Technology Device insurance program for employees

In an effort to help employees, the district is offering an opportunity to purchase an insurance policy which covers the total cost of replacing/repairing a device within the applicable terms and conditions.

Insurance Option Premiums (computer model dependent)	**Annual Fee**
Lenovo T420/T430/T440, E550, iPad2, iPad Air 32 and other staff device models below $600 initial cost	$20
Lenovo Yoga 11e Touch screen Teacher 2015 Refresh Machine and other staff device models between $601 and $999 initial cost	$25
MS Surface Pro 3, Lenovo T550/x250/T450 or other staff device models between $1000 at $1430 initial cost	$30
Any mobile device models over $1431 initial cost	$35

Employee's assigned Device:

Make/Model #_____ Device SN:_____

Device cover/case included? (Y/N) _____

Employee Name_____ Date_____

Employee School/Dept. _____ Employee ID# _____

For school/Dept. office use only (for annual device insurance option)

Funds received by: _____ *Date:* _____

Amount: _____ *Check #:* _____