



MANAGEMENT DIRECTIVE 5.01

Revision 8

DATE: May 20, 2011
TO: All Students/Parents, Visitors and Employees
FROM: Joseph G. Joyner, Ed.D., Superintendent
SUBJECT: Acceptable Use Procedures (AUP)

Introduction

The Acceptable Use Procedures (AUP) document has been moved from the District Technology Plan to this management directive to simplify distribution and streamline updates by the Superintendent as needed. It is expected that any follow-on updates will be authorized by the Superintendent.

The St. Johns County School District (SJCSD) can provide students, visitors and employees with access to the District's Voice and Data Network, which may include the Internet, e-mail, and telephone access, and any future electronic digital communication devices. Internet service is obtained through the Florida Information Resource Network (FIRN) or through commercial telecommunication carriers. The digital network (including all equipment and computers at all district sites) is the property of the St. Johns County School District and is to be used for the purpose of educating students and conducting school business as outlined in the procedures contained in this AUP.

The proper use of the Internet and digital network, and the educational value to be gained from proper Internet use, is the joint responsibility of students, parents, visitors and employees of the school district.

Purpose

The AUP provides guidelines to 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. The AUP also provides guidelines for public web content publishing. It does not outline expectations for technology integration or instruction.

Acceptable Use Procedures (AUP) Sections:

Employee, Student/Parent, and Visitor Guidelines

Web Page Guidelines

Acceptable Use Procedures Forms

- Acceptable Use Procedures (AUP)
- Waiver for Personal Electronic Property

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

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

Acceptable use of the digital network shall:

- Support education and research consistent with District Strategic Plan and curriculum goals.
- Reflect behaviors consistent with the six pillars of CHARACTER COUNTS! Trustworthiness, Respect, Responsibility, Fairness, Caring, and Citizenship.
- Be consistent with the district rules appropriate to network access.
- Not violate any of the prohibited activities.
- Require that students/parents, employees and visitors 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.
- Require that any employees, students or visitors who wish to bring any personally owned devices or other electronic property to district schools or offices first obtain permission by completing the *Waiver for Personal Electronic Property* form contained in this Acceptable Use Procedure. In addition they must sign this AUP.

2. Prohibited Activities

- 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 use related to a violation of applicable codes of conduct.
- Any fraudulent or deceptive use.
- Installation and use of any software that contains or comes bundled with spyware, adware, or other malicious code, or is deemed inappropriate or non-necessary for official school district functionality or use.
- Unauthorized use of utilities or software applications that interfere, disrupt or gather information about remote district owned network or technology resources.
- Users must not offer network infrastructure services such as DHCP, Dynamic Host Configuration Protocol, and DNS, Domain Name Service.
- Unauthorized modification or repair of School District owned technology resources and network infrastructure.
- Subverting, attempting to defeat or disabling 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.
- Users must not offer alternate methods of access to St. Johns County School District technology resources such as modems and virtual private networks (VPN's).
- Computing resources are not to be used for commercial purposes or for personal financial or other gain.
- Violating terms of applicable software purchase, licensing, or acquisition agreements or infringing any patent, copyright, trademark, or other intellectual property right.
- Use of remote access software or services to access remote computer networks, workstations or servers from district owned technology resources.
- Use of file sharing software and or services to access or share files, folders or other digital information.

- Use of internet conference or web video conferencing software or services that transmit unauthorized student images, video or other identifiable information to remote users.
- Publishing, altering or deleting code, content, or data without appropriate authorization.
- Publishing defamatory, scandalous, illegal, harassing, bullying, threatening, intimidating, or unlawfully obtained matter, or matter provoking or promoting violence.
- Willfully transmitting damaging agents (e.g., computer viruses, Trojan horses, worms) or otherwise willfully damaging or disrupting any computer facility, software, or data.
- Willfully accessing or attempting to access protected data, files, web pages, or computers (wherever located) without appropriate access rights.
- Willfully performing an act that is likely to interfere with the operation of computers, terminals, peripherals, or networks.
- Open telephone or data transfer connections.
- Willfully acting in such a manner as to bring disrepute to the St. Johns County School District, or any of its faculty, students, staff, or others.
- Willfully publishing or displaying material that injures or invades the privacy of others.
- Setting up or maintaining private servers without explicit written permission from St. Johns County School District Information Technology Department.
- Purposeful use or experimentation with software or hardware that is known to cause inoperability or downtime.
- Any use specifically prohibited by the Chief Information and Technology Officer or his or her designee after written warning.
- Users of the digital network understand there are Federal and State laws prohibiting spam mail, unsolicited mail or mass mail or chain letters. Users will not monopolize Internet access or negatively affect the bandwidth in any manner that transcends normal computer use.
- Using technology resources for political lobbying or other forms of political support.
- Using technology resources to advertise products or services that are not approved by the School Board.
- Willfully publishing, storing, displaying, transmitting, playing, or editing material that is obscene, threatening or otherwise inappropriate.
- Schools and district departments are not authorized to setup, configure, operate or provide any public server based services which include and are not limited to: Domain Name Service, Web, File Transfer Protocol, RTSP, ICQ (chat) and the like.
- Willfully changing, deleting or modifying Internet browser settings with the intent to hide or delete Internet history or records of Internet use.

3. Enforcement

Users 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 possible expulsion or dismissal. Alleged violations will be handled through the St. Johns County School District disciplinary procedures applicable to the user.

The St. Johns County School District may suspend, block or restrict access to an account or user, independent of these procedures, when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of St. Johns County School District or other computing resources or to protect the St. Johns County School District from liability. The St. Johns County School District may also refer suspected violations of applicable law to appropriate law enforcement agencies.

The St. Johns County School District reserves the right to disallow access to technology resources in order to protect the technology resources owned by the school district. In addition to this, the school district reserves the right to uninstall any software which interferes with the functionality,

security or integrity of school district owned workstations and other technology resources. The school principal or district department director will be notified if any actions are taken. Users of district owned technology resources are responsible for the security and safe-keeping of these resources at all times. Also, users can be held responsible for violations of this AUP if their system is used with or without their permission to violate any portion of this AUP or any applicable codes of conduct or laws.

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

4. No Expectation of Privacy

As providers of the computer equipment and digital network, federal and state laws give the district the right to monitor all users' communications on the district's digital network, even with remote equipment. This statutory authority is based on ensuring the appropriateness of district communications so that random computer checks may be done. Each user must have written acknowledgement of clearly understanding this procedure. The act of annually signing this document signifies the user clearly understands the procedure and agrees to execute this procedure in good faith.

5. Public Records

Each user of St. Johns County District School's Digital Network (and other resources) recognizes that he/she is 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 only. Any email accounts or software which is not considered district standard will not be supported or maintained by school district technology staff or resources.

A. User Responsibilities

- Your St. Johns County School District e-mail account is for your use only. You must not let anyone else use your account. You are responsible for all activities that originate from your computer 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 comply with all rules and regulations posted in school computer areas. You must also follow all rules established for remote networks you access.
- You must use your correct name to identify your account, either when you apply for an account or first use an account that was provided by district staff. All other personal information must be supplied when requested and must be correct and current.
- 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).

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 record data.
- Personal business or personal communications that are not work related.

C. Use of Personal E-mail, Text Messaging, Blogging/Chatting or other Web based and mobile electronic communications

For the basis of discussion, the term “text based communication” noted in this document refers to all forms of electronic communication available via the Internet or mobile devices and includes: blogging, web chat or Instant Messaging (IM), Twitter, text messaging, mobile based chat, Short Message Service (SMS), Multimedia Message Service (MMS) and the like.

- Employees are authorized to use their personally owned equipment (including mobile devices) to access personal email or text based communication only during non-duty times such as authorized lunch or break times.
- Students are only authorized to use or access personal email or webmail using district resources when it is required to register or participate in school approved online applications or courses.

- Employees should not use personal email to conduct school or district related business communications. Likewise, district email should not be used for personal business.
- Employees are not authorized to send any sensitive or protected student or staff data via personal email or text based communication. Sensitive or protected data includes elements such as: student grades, student GPA's, student incidents, student discipline issues, student FCAT scores, student assessment scores, employee or student SSN's, employee or student medical data, etc.

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. Additionally, no chat room or bulletin boards will be accessed for sending, forwarding, uploading, or downloading unless they directly support the district curriculum. These forums are considered open areas for administrative or criminal investigations, and users have no expectation of privacy.

No chat room or bulletin board will ever be used as a forum for negative, offensive, harassing, illegal or defamatory discussions. List Servers (Listservs) are not supported, hosted or maintained.

8. Copyright Infringement

Users of the digital network may not upload, download, transmit to another computer, print a hard copy or commit any infringement upon the exclusive rights of reproduction, distribution, adaptation, public performance and public display of an on-line or off-line copyrighted work. Not all works on the Internet or intranet are in the public domain. Users must check with the attorney or Media Services Department if there is any uncertainty whether an article or software is copyrighted. Additionally, it is a violation of the Digital Millennium Act to remove any copyright management information. There are serious civil and criminal penalties for violating the Federal copyright laws and international copyright treaties.

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. Trademark infringement carries stiff civil and criminal penalties.

10. Passwords

Passwords are for internal use and are not to be distributed to anyone without expressed permission of the Chief Information and Technology Officer. Employee (teacher/administrator/district staff) system or district application passwords shall not be shared with or disclosed to students, interns, other employees, visitors or friends. System or district application passwords include access to the St Johns network (STJOHNS) or other district applications (TERMS, eSIS, Oracle, PATS, FirstClass, HR Portal, ESE, etc.). Passwords are tracked for accountability and security to a specific user. Passwords do not create an expectation of privacy when it comes to employer monitoring and internal or criminal investigations.

11. Remote Use of Computers

Use of computers away from the traditional school sites includes, but is not limited to, home, car, hotel, and other off-site locations. Users shall have no expectation of privacy when conducting

school business at off-site locations. 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 will trigger civil and criminal penalties (known as spoliation claims). If users' equipment is subpoenaed or litigation is anticipated, contact the in-house attorney or Human Resources Department for guidance on how to proceed.

13. Modification or Repair of District Technology Devices and Network Infrastructure Equipment

Users must not attempt to implement, configure, or create their own network infrastructure. 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. Users must not offer or configure alternate methods of access to St. Johns County School District technology resources by using modems and virtual private networks (VPN's) or by other means. Users must not offer or configure network infrastructure services such as Dynamic Host Configuration Protocol and Domain Name Service. Exceptions to this procedure must be approved in writing by the Chief Information and Technology Officer.

Users shall not attempt to repair or modify district owned technology resources. All requests for repair or service shall be forwarded to the school or district technology support personnel for resolution. Those 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 to perform any kind of maintenance, repair, configuration or installation services to support district owned technology devices.

14. The Use and Operation of Personally Owned Technology Devices or Electronic Property

Students, staff and visitors who are authorized to use or operate personally owned devices must adhere to the following:

- 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.

- Students or staff 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.
- Employees who wish to use their personal technology equipment to access personal email, text based messages or voice communication, please refer to section (6c) in this document.

15. Terms and Conditions

All terms and conditions as stated in this Acceptable Use Procedure are applicable to all users of the network and district technology equipment.

Any violation of the Acceptable Use Procedure could lead to the revocation of the network and computer access privileges, disciplinary action and/or appropriate legal action as outlined in Section 3, Enforcement, of this procedure.

16. Amendments

This procedure may be amended or revised from time to time as need arises. Users will be provided with copies of all amendments and revisions.

17. Additional Requirements for Students/Staff/Visitors Requesting a Waiver for Personal Electronic Property

Students, staff and visitors requesting to operate their personal electronic property within the district must obtain written approval and abide by the following additional requirements:

- 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.
- A Waiver for Personal Electronic Property form must be signed (denoting approval) by the school or district department administrator prior to operating any personal electronic property in St. Johns County School District schools or offices.
- Any visitor/student/staff that operates any personal electronic property must also sign and acknowledge this AUP.

18. Additional Guidelines for Students

Student users must adhere to the following additional guidelines:

- Students will follow teacher instructions regarding the use of the St. Johns County digital network.
- Students must observe and adhere to all regulations when using any digital device on school campus or during sponsored events including cell phone use as outlined in the Student Conduct Code.

19. Additional Requirements for Teachers/Administrators

Teachers, administrators and all other 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.
- Student use of teacher or administrative computer systems that access district applications or network and data resources is prohibited.
- Teachers and administrators are responsible for the safe keeping of all content (data security) and appropriate use of the system at all times.
- Teachers and administrators 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/depts/it/awareness>).
- 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.
 - Teachers, school staff and district staff should avoid using personal email, personal websites (including personal blog websites), and social networking websites to communicate school related information to students or parents.
 - Teachers, school staff and district staff who communicate with students or parents by any means, must comply with the Florida Education Profession Code of Ethics and Principles of Professional Conduct for the Education Profession. Below is the link to the Florida DOE Office of Professional Practices:
http://www.fldoe.org/edstandards/code_of_ethics.asp
 - Text based communications between students and school staff should only be used to relay time sensitive critical messages (typically dealing with event attendance or participation).
 - Teachers, school staff and district staff should communicate with students/parents using the tools and systems provided by the District, such as District Email, District websites, Teacher websites, eSIS Parent Assistant, or by work phone and in person.
 - Teachers, school staff and district staff should take great care when communicating with parents via district email that contains protected student data (such as discussing grades or behavior problems or assessment results) because email is generally unsecure. Instead, communicate details via phone, Parent Assistant online or at a parent conference, all of which offer far better security.
 - Teachers, school staff and district staff 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.



20. **Additional Requirements applicable to Teachers, Administrators, Visitors and Students**

The Use of Audio and/or Video Recording and Recording-Capable Devices

This section covers the use of any device that can record audio or video in the school environment, particularly the classroom. All students, staff and visitors must adhere to the following:

- Students may possess instructional technology devices that record audio and/or video and utilize them as instructional tools in the classroom only with the consent and under the direction of the school administration and teacher, as it pertains to the current curricular unit, lesson etc.
- All active recordings must be disclosed to all parties present during recording.
- No hidden recording devices are permissible.
- All recording devices must be powered off when not in use.
- Publication of recordings without prior written consent from the Principal is prohibited.
- Recordings have the potential to inadvertently capture the transmission of copyrighted materials. All copyright and intellectual property laws and restrictions apply.
- Recording of private conversations without agreement by all parties is strictly prohibited.
- All recordings must be in compliance with state and/or federal recording and/or wiretapping laws.
- Recording of public events is allowed where permissible by Florida law.

Examples of Recording and Recording-Capable Devices include, but are not limited to:

- Smart Pen (i.e. Livescribe Echo)
- Personal audio recorder (i.e. Olympus Digital Voice Recorder)
- Mobile Phone or Smart Phone (i.e. iPhone)
- Personal Media Player/MP3/MiniDisc Player (i.e. iPod)
- Tablet or Slate Device (i.e. iPad)
- eReader (i.e. NookColor)
- Computer System (i.e. notebook, netbook, etc)
- Digital Still Camera (i.e. Canon Powershot SD1300is)
- Digital Video Camera (i.e. Flip UltraHD)
- Tape-based Video Camera
- Tape-based Audio Recorder (i.e. Cassette player)

21. 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 other AUP violations) 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 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 an Internet safety course or lecture each year before using school computers. This course will instruct students on how to safely search the Internet, what "not to" search for (or avoid), some of the dangers the Internet poses, why filters are in place and what can happen if these procedures are not followed. Students will also be familiar with the AUP and be responsible for good choices. Students are responsible to understand the consequences of violating the AUP.
- 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 AUP.
- The District should standardize student AUP violation penalties across all schools. AUP violations are subject to consequences governed in the SJCS Student Code of Conduct.

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 server to host their website.

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 property and must adhere to procedures and guidelines of the Acceptable Use Procedure for the St. Johns County School District Digital Network.

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 advertising or [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. The school webmaster is responsible for approving all published web content.

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

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 on School and District Websites

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

Student photographs, drawings, and written work that are published on a class or school web page also must NOT contain any personal information that can be linked to the student. Teachers may use first names or other codes, such as the teacher's name and a number for each student, within the web page and with all file names.

If a student's picture is accompanied by other identifiable data (including full name, address or names of parents/relatives, etc.) and is to be published on the Internet or transmitted outside of the district, parent or guardian permission is required. Parent or guardian permission is granted by completing and signing the *School Registration Form*.

5. Publishing Student Information Including Photos 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.

- Direct web links from a school or district web site to any commercial web site for the purpose of fundraising is prohibited.
- 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. Online Grade Books

All schools are encouraged to use the District's online eSIS grade book. Many schools are required to use the District's online eSIS grade book to support the Parent Assistant program. All high schools, middle schools and selected elementary schools will continue to participate in the eSIS Parent Assistant program for the 2011-2012 school year. This module of eSIS allows parents to see their child's grades, absences, courses, assignments and much more. To enable this functionality, teachers must use the eSIS online grade book.

Schools that do not wish to use the eSIS grade book may elect to use a commercial product that is capable of calculating, tracking and publishing student grades provided that no identifiable and traceable student information is released to the public or the grade book vendor. These grade book applications can export student grades in a format which can be posted to school websites and be accessed by parents. All published grade information shall contain no student identifiable information. For example, each student could be given a random number (not SSN or name). This way if the information is compromised or viewed by the public, no data could be traced back to any student. Care must be taken to select a website service that follows instructional best practices in publishing web content.

9. Respecting Copyright

Copyright will be respected. The author of the web page will not use copyrighted materials without permission.

10. Claiming Copyright

Copyright may be claimed by the author for original work. The SJCS D Acceptable Use Procedure clearly states that there is to be no commercial use of the district's Internet connection.

11. 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.
- Site-wide navigation linking to the key areas of the school website.
- The name of the school inside the <TITLE> tag.

These items will be managed by the school 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.

12. 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 50 kilobytes 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 posting documents exceeding 2 megabytes in size.
- 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.
- 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.

13. Web Content Developed by Staff

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. All teacher web pages shall be approved by each school's webmaster.

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 covered in Management Directive 5.04.

14. 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. Student photographs, drawings, and written work that are published on a class or school page may NOT contain any personal information that can be linked to the student. Teachers may use first names or other codes, such as the teacher's name and a number for each student within the web page and with all file names.

The following procedures apply:

- Student web pages which profile a student are prohibited. No web page shall contain a student's phone number, address, e-mail address, opinions, or other personal information.
- Students may create "content" pages, under their instructor's supervision, pertaining to class, events, or activity.
- Students, who create blog content, podcasts or videos must comply with this AUP, follow the direction and supervision of their instructor and be used for educational purposes.
- Blogs in use by St. Johns County School District students must be registered with their local school or department with an accountable publisher and content approver who is responsible for 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.

15. 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.

Acceptable Use Procedures Agreement Form

(Applies to visitors, employees and students who wish to use the District's Digital network)

Upon signing this agreement, I, a user of the digital network, acknowledge that I clearly understand the agreement and have no further questions as to the content and delivery of this Acceptable Use Procedure and agree to abide by agreement.

I, as a user of the Digital Network, also affirm that since I have no confusion over the content of this procedure, there will be no violation of this procedure or any other civil nor criminal laws relating to computer use.

I, as a user of the Digital Network, will indemnify the St. Johns County School District and hold harmless for violating St. Johns County District Schools Digital Network Acceptable Use Procedure which causes: 1) humiliation internally and with the public; 2) disruption of services; and, 3) civil or criminal liability.

I, as a Digital Network Acceptable Use Procedure user, waive any right to litigate an inadequate training claim or other negligence claim against St. Johns County Schools for not clearly understanding this procedure.

I understand that the written portion of the Acceptable Use Procedure must be signed annually by every St. Johns County School District employee, student/parent or external user. This written agreement for use and access to the St. Johns County School District Digital Network will be required in writing and kept on file at each school or district department.

Employee, Student or External User (Visitor) (Applies to all users)

User Name (please print): _____

School/Department or Visitor Affiliation: _____ (i.e., SAHS, IT Dept., Parent, Newspaper)

User Signature: _____ Date: _____

Parent/Guardian Permission (Required for students to operate or access District technology resources)

As the parent or guardian of this student, I have read, understand, and agree to the school district procedures relating to acceptable use of the St. Johns County School District Digital Network and the Internet. I hereby give permission for my child to use the St. Johns County School District Digital Network using the aforementioned procedures and certify that the information contained on this form is correct.

Parent/Guardian's Name (please print): _____

Parent/Guardian's Signature: _____ Date: _____

Administrator's Approval (School or District Department Designee) (Applies to all users)

The administrator verifies the user and approves their access to the St. Johns County School District Digital Network.

Administrator's Name (please print): _____

Administrator's Signature: _____ Date: _____

Waiver for Personal Electronic Property Form

(Applies to employees, students or visitors who wish to use personal electronic equipment at school or district offices)

This is an agreement, applicable to students, staff and visitors, to be responsible and accountable users of any personal electronic property they wish to bring onto School or District premises.

I wish to petition the St. Johns County School District Administration to be allowed to bring the specified portable computer or small form factor device, also know as a Personal Digital Assistant, to the District Office or School requested below. I understand that this device is my personal property and not the property of the School or District. As such, I understand that SJCS D can assume no responsibility for this device and will be held blameless in the event of damage or loss. I understand that responsibility for the care of the device AND my behavior while using this device belongs solely to me.

As a user of the St. Johns County School District computer network, I agree to comply with the AUP requirements regarding additional requirements for visitors/students/staff requesting a waiver for Personal Electronic Property, in addition to the AUP requirements for network use.

Employee, Student or External User (Visitor) (Applies to all waivers)

User Name (please print): _____

Requested Device(s): _____

School/Department or Visitor Affiliation: _____ (i.e., SAHS, IT Dept., Parent, Newspaper)

User Signature: _____ (Not required for students) Date _____

Parent/Guardian Permission (Required for students to operate personally owned technology devices in school or on school property)

As the parent or guardian of this student, I have read, understand, and agree to the school district procedures relating to acceptable use of personal electronic property. I hereby give permission for my child to use the specified electronic device on the St. Johns County School District Digital Network using the aforementioned procedures and certify that the information contained on this form is correct.

Parent/Guardian's Name (please print): _____

Parent/Guardian's Signature: _____ Date _____

Administrator's Approval (School or District Department Designee) (Applies to all waivers)

The administrator verifies the user and approves their access to the St. Johns County School District Digital Network.

Administrator's Name (please print): _____

Administrator's Signature: _____ Date _____

Technology Equipment Responsibility Form

(Applies to district employees assigned technology equipment)

By signing this form, the undersigned acknowledges full responsibility for all information listed. Each item listed should be initialed. Technology equipment and devices are also referred to as district assets. The most common form of technology equipment assigned to teachers and staff members are notebook computers. In addition, the undersigned agrees to waive any right to litigate an inadequate training claim or other negligence claim against St. Johns County Schools for not clearly understanding this procedure.

Initial each item below: *(Applies to all employees assigned District Technology equipment)*

1. _____ I agree to comply with the St. Johns County School District Acceptable Use Procedures.
2. _____ I acknowledge responsibility for asset's physical condition.
3. _____ I acknowledge responsibility for physical security of the asset.
4. _____ I acknowledge responsibility for security of data stored on asset.
5. _____ I acknowledge that use of asset is not authorization for overtime eligible employees.
6. _____ I have read and understand the guidelines listed below referring to lost, stolen or damaged technology equipment that is assigned to me:
 - a. Employees found to be negligent for lost, stolen or damaged technology equipment are responsible to pay the District's net book value for that device but no lower than \$250.00.
 - b. Employees agree to write a personal check (or money order) or have the charges deducted from their paycheck either as a one-time deduction or spread over four (4) paychecks.
 - c. Employees found liable further agree to pay the district in full or begin payments within 30 days of notification but no later than the end of the school year whichever is sooner.

Employee Name		Date	
School or Department			
Supervisor Name			
Technology Equipment (or device) Information			
Asset Type + any peripherals (i.e. notebook computer w/case)			
Manufacturer		Model	
Serial Number		District Asset Number	
Employee Signature		Date	

Student Technology Asset Assignment Procedures

These procedures cover the guidelines and requirements for assigning technology assets to students for individual and/or home use. A signed Student Technology Asset Responsibility Form (available on next page) must be on file before an asset can be assigned to a student for use.

Guidelines and Requirements for Students that are assigned Technology Assets

- I. Each student must have a signed Acceptable Use Procedures (AUP), Student Technology Asset Responsibility Form and any applicable St. Johns County School District (SJCS D) property or inventory forms on file.
- II. Not all students are provided a system for individual use.
- III. Systems are assigned for a maximum of one school year. This agreement must be renewed and the asset must be reassigned annually.
- IV. School or department that assigns the system to a student must obtain the signatures on the asset responsibility form. No system should be assigned without a signed AUP, Responsibility Form and any applicable SJCS D property forms on file.
- V. Systems provided for student use are intended to support learning. These systems are not provided for any individual's personal (non-school related) use. System should not be used by other students, family members or individuals.
- VI. Systems provided for student use are provided as-is. SJCS D cannot be held responsible for lost productivity or data loss that may occur if the system is improperly used or if the software or hardware malfunctions.
- VII. SJCS D cannot guarantee the security of the asset when it is not on the SJCS D network. Use of this system on other networks (home network, public wifi, etc) may result in unwanted access and exposure to material that is not appropriate for student-age individuals. Students should be supervised by a parent or guardian when using the system outside of the SJCS D network.
- VIII. Any violation of the SJCS D AUP may result in the asset being recalled from a student for examination. If AUP violations are discovered the system may be reconfigured with more restrictive security settings or recalled indefinitely.
- IX. Personal software and media should not be installed or stored on any SJCS D systems.
- X. SJCS D systems assigned to individuals may be requested to be brought to a school or district department periodically for routine maintenance and updates to be performed. Individuals assigned systems should make a reasonable effort to return the system in a timely manner if requested. Refusing to return the asset will be considered a violation of the district AUP and may result in the system being recalled indefinitely.
- XI. Systems may be configured with District software – including security software. Any attempt to remove, modify or disable District applications is strictly prohibited. Installation of personal software is also prohibited (see item IX).
- XII. Support for systems is limited. Support requests must be coordinated by the department or school that provides the system. Support for systems may require that systems be returned to a school or district department for diagnosis and repair.
- XIII. A signed Student Technology Asset Responsibility Form and any applicable SJCS D Property/Inventory form must be completed for each asset that is assigned to a student for individual use.

Student Technology Asset Responsibility Form

(Applies to parents of students who are assigned district technology assets or equipment)

By signing this form, the undersigned acknowledges full responsibility for all information listed. Each item listed should be initialed by a parent or guardian of the student that the asset is being assigned to. In addition, the undersigned agrees to waive any right to litigate an inadequate training claim or other negligence claim against St. Johns County Schools for not clearly understanding this procedure.

Parent or Guardian must Initial each item below if student is under 18 years of age. Student and Parent or Guardian will:

1. _____ Follow all parts of St. Johns County School District Acceptable Use Procedures (AUP) also called Management Directive 5.01.
2. _____ Acknowledge responsibility for asset's physical condition.
3. _____ Safeguard and provide for physical security of the asset.
4. _____ Follow all parts of the Student Asset Assignment Procedures.
5. _____ Read and understand the guidelines listed below referring to lost, stolen or damaged devices:
 - a. Individuals found to be negligent for lost, stolen or damaged devices are responsible to pay market value for that device.
 - b. Individuals agree to write a personal check (or money order) to pay for a lost, damaged or stolen system.
 - c. Individuals found liable further agree to pay the district in full or begin payments within 30 days of notification but no later than the end of the current school year whichever is sooner.

Student Name <i>(First, Middle Initial, Last)</i>			
Assigning School or Department		Student Grade Level	
Assigning Administrator <i>(Print)</i>		School Year	
Asset Information	Asset Type		
Manufacturer		Model	
Serial Number		Asset Number	
Parent or Guardian Name <i>(Print)</i>			
Parent or Guardian Signature		Date	