Acceptable Use Policy (AUP) and Internet Safety Policy Guidelines for Students and Visitors

GUIDELINES AND PROCEDURES FOR STUDENTS/VISITORS OF ST. JOHNS COUNTY SCHOOL DISTRICT DIGITAL NETWORK AND TECHNOLOGY RESOURCES

1. Internet Safety

The following policy guidelines are in place to protect students and visitors:

- **Prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications.**
  - To the extent practical, technology protection measures (or "Internet filters") shall be used to block or filter Internet, or other forms of electronic communications, access to inappropriate information.
  - Specifically, as required by the Children's Internet Protection Act, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors.
  - Subject to staff supervision, technology protection measures may be disabled for adults or, in the case of minors, minimized only for bona fide research or other lawful purposes.
  - The use of (or access to) TikTok or any successor platforms is prohibited on District devices and District network infrastructure (District Internet/WiFi).
- **Prevent unauthorized access and other unlawful online activity.**
  - To the extent practical, steps shall be taken to promote the safety and security of users of the online computer network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications.
  - Specifically, as required by the Children's Internet Protection Act, prevention of inappropriate network usage includes: (a) unauthorized access, including so-called 'hacking,' and other unlawful activities; and (b) unauthorized disclosure, use, and dissemination of personal identification information regarding minors.
- **Prevent unauthorized online disclosure, use, or dissemination of student personally identifiable information (PII).**
- **Prevent access to websites, web or mobile applications or software that do not protect against the disclosure, use or dissemination of student PII in accordance with rule 6A-1.0955 F.A.C.**
- **Provide student education, supervision and monitoring.**
  - School staff should submit a ticket to request that blocked content be reviewed and unblocked (if needed) for educational purposes.
  - Students are prohibited from accessing social media platforms, except when expressly directed by a teacher for an educational purpose.
  - School staff will educate, supervise, and monitor appropriate usage of the online computer network and access to the Internet in accordance with this policy, the Children's Internet Protection Act, the Neighborhood Children's Internet Protection Act, and the Protecting Children in the 21st Century Act.

    - Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of the IT Department.
    - Schools will provide age-appropriate training for students who use the Internet facilities. The training provided will be designed to promote the commitment to:
        i. The standards and acceptable use of Internet services as set forth in the AUP and Internet Safety Policy guidelines.
        ii. Student safety with regard to:
            1. Safety on the Internet.
            2. Appropriate behavior while on online, on social networking Web sites, and in chat rooms.
            3. Cyberbullying awareness and response.
        iii. Compliance with the E-rate requirements of the Children's Internet Protection Act ("CIPA").
        iv. Following receipt of this training, the student will acknowledge that he/she received the training, understood it, and will follow the provisions of the District's acceptable use and Internet Safety policy guidelines.
- **Comply with the Children's Internet Protection Act** [Pub. L. No. 106-554 and 47 USC 254(h)].

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

The following are typical uses of the digital network:

- Students' use of the District's digital network, internet service and other electronic resources is a privilege. As a condition of that privilege, students must comply with this Acceptable Use Policy ("AUP"). The following general rules govern students' 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 this Acceptable Use Policy ("AUP").
- The use must comply with the instructions of teachers and staff.
- The use must comport with the six pillars of CHARACTER COUNTS!
- Require that students 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 (a) bullying and harassment and (b) copyright laws.

3. Prohibited Activities

The following are prohibited:

- Use that violates the Code of Conduct.
- Use of another individual's account or providing individual account information to another person.
- Use of the network for financial gain or for political or commercial activity.
- Attempting to send or sending anonymous messages of any kind or pretending to be someone else while sending a message.

- Attempting to access, modify, harm or destroy another user's data on the network.
- Harassing, insulting, ridiculing, attacking or defaming others via network communications.
- 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.
- Users of unauthorized methods of access to St. Johns County School District technology resources such as modems and virtual private networks (VPN's).
- Use of remote access software or services to access remote computer networks, workstations or servers from the district system.
- Attempting to transmit damaging agents (e.g., computer viruses, Trojan horses, worms) or otherwise willfully damaging or disrupting any computer facility, software, or data. Attempting to interfere with the normal operation of computers, terminals, peripherals, or networks.
- Usage invades the privacy of others.
- Use or experimentation with software or hardware without written approval from the CIO.
- Willfully publishing, storing, displaying, transmitting, playing, or editing material that is obscene, threatening, profane, prurient, sexually suggestive or otherwise inappropriate.
- Changing, deleting or modifying Internet browser settings including hiding or deleting Internet history or records of Internet use.
- Use of the system for an unauthorized purpose.
- Broadcasting a WiFi signal or operating a personal Hotspots from personal devices.
- Students shall not perform any kind of maintenance, repair, configuration or installation services on District owned devices.
- The use of TikTok or any successor platforms used to communicate or promote any District or School or any District/School sponsored event/club/team/organization.

4. Enforcement

Students who violate these procedures may be denied access to St. Johns County School District computing or technology resources and may be subject to disciplinary action, including possible expulsion. Alleged violations will be subject to the St. Johns County School District disciplinary procedures.

5. No Expectation of Privacy

Students and visitors have no expectation of privacy in their use of the District system.

6. AUP Agreement and Acknowledgement

As a condition of the privilege of using the District's system and technology resources, students/parents are required to annually acknowledge and agree to the District AUP guidelines contained herein via the District's online Returning Student Verification form or the online New Student Enrollment form. AUP acknowledgement via the District's online forms (noted above) is the primary method recommended because that process also updates our student information system. The AUP form found in this document is included for illustration and can be used (if needed).

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

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

- District employees are not authorized to install software, perform any repair, configuration or maintenance on student-owned technology resources, that are brought to school property or present during school sponsored activities including both software and hardware resources.
- Students 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. The District is in no way liable for any loss or damage for student-owned devices.
- Schools/Departments will not be responsible to hold or store student-owned devices.
- The use of TikTok or any successor platform used to communicate or promote any District or School sponsored event/team/club/organization.

8. Additional Requirements for Students or Visitors Requesting a Waiver for Personal Electronic Property or Bring Your Own Device (BYOD)

Students and visitors requesting to operate their personal computing device (notebook computer, touch tablet, etc.) 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 functioning anti-virus software running with up-to-date virus definitions. Preferable antivirus 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 student or visitor that operates any personal electronic property must also sign and acknowledge this AUP.

9. 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.
- Students will comply with the St. Johns County Digital Citizenship Guidelines.

10. Additional Rules Governing the Use of Video, Photo and/or Audio Recording Devices at School

This section addresses the use of devices that can record audio, photo or video content in the school environment, particularly the classroom. Such recording 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)

General Rule.

Except at open house and public events as discussed below, students, parents and visitors are not allowed to videotape, photograph or make audio recordings while on school premises. All recording devices must be turned off at school. The purpose of this general rule is to foster an appropriate educational environment, prevent unwarranted disclosure of student images and information, and to comply with the requirements of the negotiated agreement with the St. Johns Education Association.

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.

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. The following procedures apply:

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.
- 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.

- 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.

12. Students' use of Artificial Intelligence (AI) in Schools

General AI use and precautions:

It is the School District's intention to train employees and instruct students to use AI tools in an ethical and educational way. The School District is **not** prohibiting employee or student use of AI, but each employee and student must be aware of the limitations, AI model biases, and guidelines of its use prior to using AI for work and/or educational purposes**.**

- **Students must not** share personal or sensitive data when using AI tools.
  When using an AI tool, students need to be aware that all information (personal or other) they upload when using an AI tool becomes the property of that tool and will affect their own privacy and their peers' privacy.

- **Students must acknowledge** that AI is not always factually accurate or a credible source.
  AI models have implicit and/or explicit biases and may even present incorrect information. Students should always fact check AI generated information using primary sources.

- **Students must annotate when using AI** to assist with schoolwork and assignments, including, but not limited to, generated AI text, images, multimedia, etc. The improper use of AI shall be subject to all District policies (e.g., Code of Conduct) and could result in disciplinary consequences. Academic integrity is critical to a student's success.

- **The District standard AI tool for student use is Microsoft Copilot**
  Microsoft's Copilot provides a Protected mode that will help safeguard students' data and filter responses. Other more common AI tools will be blocked from student use.

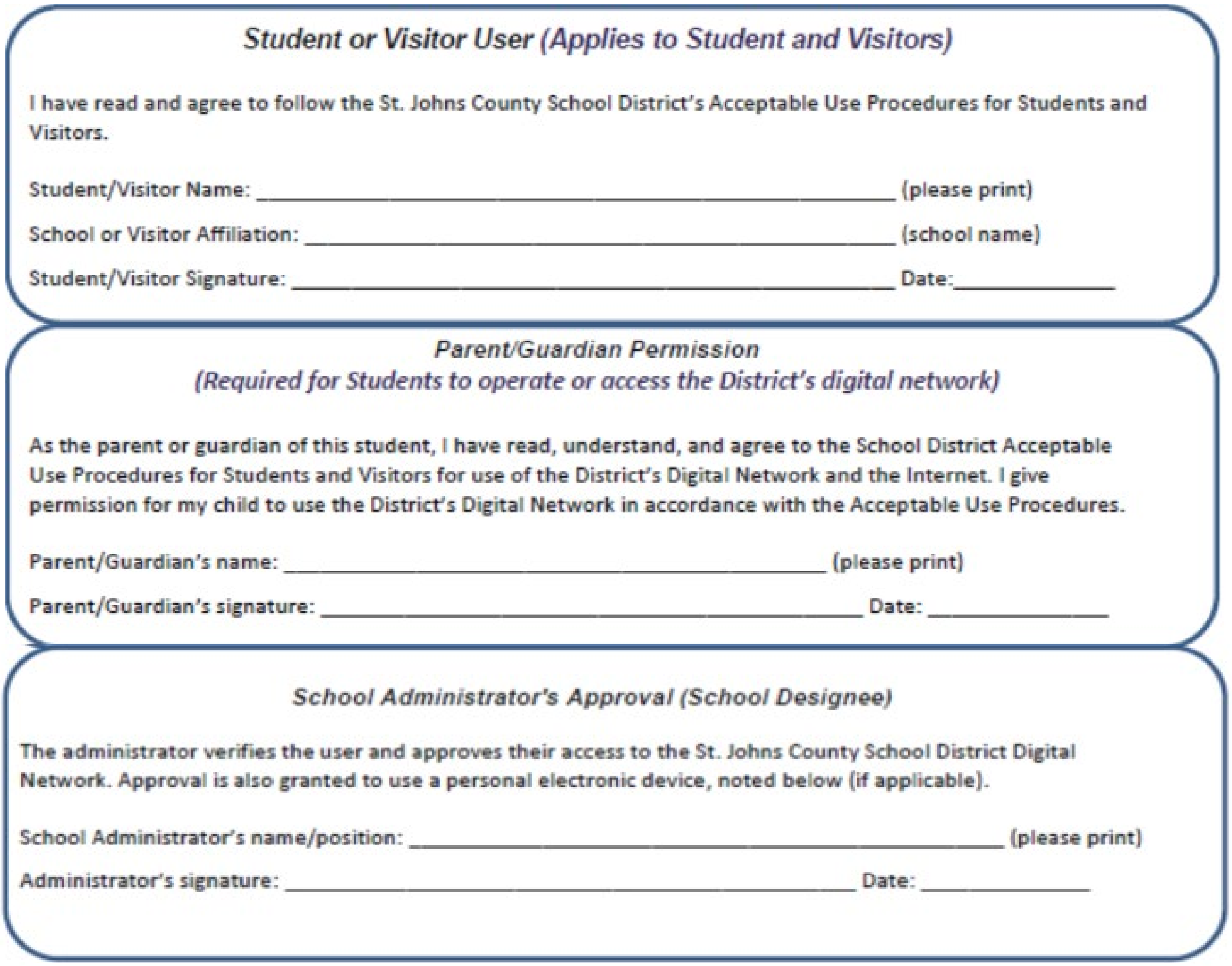
Prohibited Uses of AI by Students

- The use of AI for unlawful purposes including hacking or using AI tools to learn passwords, breach confidentiality, or expose/release Personal Identifiable Information (PII) data.
- The use of AI when it is expressly prohibited by the student's teacher to complete assigned work.
- Uploading, sharing, providing, or otherwise releasing PII data (which includes staff or student name, address, age, phone, email, place of birth, date of birth, SSN, etc.) when using AI tools.
- The use of AI that is specifically prohibited by law or not District approved.

- The use of AI to create deceptive, false, misleading, or inappropriate diagrams, photos, videos, audio or illustrations.
- Presenting AI generated work as your own.

Student/Visitor Acceptable Use Policy Agreement Form

(Applies to students or visitors who wish to use the District's digital network)
Parents typically agree to this AUP during Online Enrollment Verification or initial Enrollment.



Student or Visitor User *(Applies to Student and Visitors)*

I have read and agree to follow the St. Johns County School District's Acceptable Use Procedures for Students and Visitors.

Student/Visitor Name: ____ (please print)

School or Visitor Affiliation: ____ (school name)

Student/Visitor Signature: ____ Date:___________

Parent/Guardian Permission
(Required for Students to operate or access the District's digital network)

As the parent or guardian of this student, I have read, understand, and agree to the School District Acceptable Use Procedures for Students and Visitors for use of the District's Digital Network and the Internet. I give permission for my child to use the District's Digital Network in accordance with the Acceptable Use Procedures.

Parent/Guardian's name: _______________________________________ (please print)

Parent/Guardian's signature: ____________________________________ Date: ____________

School Administrator's Approval (School Designee)

The administrator verifies the user 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: ____________