

Avoyelles Parish School System Student Acceptable Use Policy 2023-2024

Introduction

Avoyelles Parish School System recognizes that access to technology in school gives students greater opportunities to learn, engage, communicate, and develop skills that will prepare them for work, life, and citizenship. We are committed to helping students develop 21st-century technology and communication skills.

To that end, we provide access to technologies for student and staff use.

This Acceptable Use Policy outlines the guidelines and behaviors that users are expected to follow when using school technologies or when using personally-owned devices on the school campus. The Internet safety policy addresses all of the following issues:

- Access by minors to inappropriate matter on the Internet and World Wide Web
- The safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications
- Unauthorized access including "hacking" and other unlawful activities by minors online
- Unauthorized disclosure, use, and dissemination of personal information regarding minors
- Measures designed to restrict minors' access to materials harmful to minors

- The Avoyelles Parish School System network is intended for educational purposes. It should not be used for commercial purposes, financial gain, and fraud or to engage in any illegal acts.
- All activity over the network or using district technologies may be monitored and retained.
- Access to online content via the network may be restricted in accordance with our policies and federal regulations, such as the Children's Internet Protection Act (CIPA).
- Students are expected to follow the same rules for good behavior and

respectful conduct online as offline.

- Misuse of school resources can result in disciplinary action.
- Avoyelles Parish School System makes a reasonable effort to ensure everyone's safety and security online, but will not be held accountable for any harm or damages that result from use of school technologies.
- Users of the district network or other technologies are expected to alert IT staff immediately of any concerns for safety or security.

Technologies Covered

Avoyelles Parish School System may provide Internet access, desktop computers, mobile computers or devices, videoconferencing capabilities, online collaboration capabilities, chat rooms, message boards, email, and more.

As new technologies emerge, Avoyelles Parish School System will attempt to provide access to them. The policies outlined in this document are intended to cover *all* available technologies, not just those specifically listed.

Terms and Conditions

Usage Policies

- All technologies provided by the district are intended for education purposes.
- All users are expected to use good judgment and to follow the specifics of this document as well as the spirit of it: be safe, appropriate, careful and kind; don't try to get around technological protection measures; use good common sense; and ask if you don't know.

Web Access

- Users are expected to respect that the web filter is a safety precaution, and should not try to circumvent it when browsing the Web.
- If a site is blocked and a user believes it shouldn't be, the user should inform a teacher.

Social/Web 2.0 / Collaborative Content

Recognizing the benefits collaboration brings to education, Avoyelles Parish School System may provide users with access to web sites or tools that allow communication, collaboration, sharing, and messaging among users.

- Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline.
- Posts, chats, sharing, and messaging may be monitored.
- Users should not use full names when online. Use either your first name and last initial or first initial and last name.
- Regardless of the privacy settings, assume that all information shared online is public information and always remember that you are a representative of the Avoyelles Parish School System.
- Online conversations are never private so personally identifying information like first and last name, birth date, cell phone number, and address and information about personal schedules should never be shared.

Mobile Devices Policy

Avoyelles Parish School System may provide users with mobile computers or other devices to promote learning outside of the classroom.

- Users should abide by the same acceptable use policies when using school devices **off the school network as on the school network.**
- Users are expected to treat these devices with extreme care and caution; these are expensive devices that the school is entrusting to your care. Users should report any loss, damage, or malfunction to IT staff immediately. **Users may be financially accountable for any damage resulting from negligence or misuse.**
- **Use of school-issued mobile devices off the school network may be monitored.**

Personally-Owned Devices Policy

- **Students must notify the technology coordinator at his/her school when bringing a**

personally-owned device so that it can be checked for the appropriate settings and an antivirus program prior to joining the school network.

- Students should keep personally-owned devices (including laptops, tablets, smart phones, and cell phones) turned off and put away during school hours—unless in the event of an emergency or as instructed by a teacher or staff for educational purposes.
- Because of security concerns, when personally-owned mobile devices are used on campus, they should have the proper antivirus programs prior to joining the school network.

Security

- Users are expected to take reasonable safeguards against the transmission of security threats over the school network. This includes not opening or distributing infected files or programs and not opening files or programs of unknown or untrusted origin.
- If you believe a computer or mobile device you are using might be infected with a virus, please submit a work order ticket to the school's technology coordinator. Do not attempt to remove the virus yourself or download any programs to help remove the virus.
- Users should not log on or attempt to log on as school staff, including teachers, librarians, and administrators.
- Users should always log out of online accounts when stepping away from the computer to ensure the safety of personal information and to protect against others using your account falsely to post any information.
- Users are responsible for account information and passwords and should take every precaution to keep these private. You should not give your password to anyone else nor post it in written form where it can be viewed by others.

Netiquette

- Users should always use the Internet, network resources, and online sites in a courteous and respectful manner.

- Restrictions against inappropriate language apply to public messages, private messages, and material posted on web pages.
- Users should recognize that although there is valuable content online, there is also unverified, incorrect, or inappropriate content.
- Users should use trusted sources when conducting research via the Internet.
- Users should also remember not to post anything online that they wouldn't want parents, coworkers, or employers to see. Once something is online, it's out there—and can sometimes be shared and spread in ways you never intended.

Plagiarism

- Users should not plagiarize (or use as their own, without citing the original creator) content, including words or images, from the Internet.
- Users should not take credit for things they didn't create themselves, or misrepresent themselves as an author or creator of something found online.
- Research conducted via the Internet should be appropriately cited, giving credit to the original author.

Personal Safety

- Users should never share personal information, including phone number, address, social security number, birthday, or financial information, over the Internet without adult permission.
- Users should recognize that communicating over the Internet brings anonymity and associated risks, and should carefully safeguard the personal information of themselves and others.
- Users should never agree to meet someone they meet online in real life without parental permission.
- If you see a message, comment, image, or anything else online that makes you concerned for your personal safety or you feel is inappropriate, bring it to the attention of an adult (teacher or staff if you're at school; parent if you're using the

device at home) immediately.

Cyberbullying

Cyberbullying will not be tolerated. Instances of cyberbullying will be reported to law enforcement.

- Name-calling, taunting/ridiculing, mocking, making offensive comments, and teasing are all examples of bullying. Cyberbullying can occur through offensive text messages, sending degrading images, posting rumors or lies, or assuming a person's electronic identity with the intent of causing harm.
- Engaging in these behaviors, or any online activities intended to harm (physically or emotionally) another person, will result in severe disciplinary action and loss of privileges.
- In some cases, cyberbullying can be a crime. Remember that activities are monitored and retained. It is staff's responsibility to handle cyberbullying following district policy.

Examples of Acceptable Use

I will:

- ✓ Use school technologies for school-related activities.
 - ✓ Follow the same guidelines for respectful, responsible behavior online that I am expected to follow offline.
 - ✓ Treat school resources carefully, and alert staff if there is any problem with their operation.
 - ✓ Encourage positive, constructive discussion if allowed to use communicative or collaborative technologies.
 - ✓ Alert a teacher or other staff member if I see threatening, inappropriate, or harmful content (images, messages, posts) online.
 - ✓ Use school technologies at appropriate times, in approved places, for educational pursuits.

- ✓ Cite sources when using online sites and resources for research.
- ✓ Recognize that use of school technologies is a privilege and treat it as such.
- ✓ Be cautious to protect the safety of myself and others.
- ✓ Help to protect the security of school resources.
 - ✓ Inform school authorities of any message received that is inappropriate. This is not intended to be a comprehensive list. Users should use their own good judgment when using school technologies.

Examples of Unacceptable Use

I will not:

- ✓ Use school technologies in a way that could be personally or physically harmful.
- ✓ Attempt to find inappropriate images or content.
- ✓ Engage in cyberbullying, harassment, or disrespectful conduct toward others.
- ✓ Try to find ways to circumvent the school's safety measures and filtering tools.
- ✓ Use school technologies to send spam or chain mail.
- ✓ Plagiarize content I find online.
- ✓ Post personally-identifying information, about myself or others.
- ✓ Agree to meet someone I meet online in real life.
- ✓ Use language online that would be unacceptable in the classroom.
- ✓ Use school technologies for illegal activities or to pursue information on such activities.
 - ✓ Attempt to hack or access sites, servers, or content that isn't intended for my use.

This is not intended to be an exhaustive list. Users should use their own good judgment when using school technologies.

Limitation of Liability

Avoyelles Parish School System will not be responsible for damage or harm to persons, files, data, or hardware.

While Avoyelles Parish School System employs filtering and other safety and security mechanisms, and attempts to ensure their proper function, it makes no guarantees as to their effectiveness.

Avoyelles Parish School System will not be responsible, financially or otherwise, for unauthorized transactions conducted over the school network.

Violations of this Acceptable Use Policy

Violations of this policy may have disciplinary repercussions, including:

- Suspension of network, technology, or computer privileges
- Notification to parents
- Detention or suspension from school and school-related activities
- Legal action and/or prosecution

I have read and understood this Acceptable Use Policy and agree to abide by it:

Student Name

Student Signature

Date

I have read and discussed this Acceptable Use Policy with my child:

Parent Name

Parent Signature

Date