STUDENT ACCEPTABLE USE POLICY

Using technology is a privilege, and any privilege comes with responsibility. Below are the expectations for using technology in the Wentzville R-IV School District (the "District"). These expectations apply when using District technology—whether on campus or remotely—and cover all devices, accounts, and online services provided by the District.

Learning and curiosity

I understand that school technology and networks are provided to help support my learning and curiosity.

- I will use technology to learn new things.
- I will use technology to complete assignments and other school activities.
- I will use my device to research and check the accuracy of information.
- I will give credit to the creators of any content I use that is not my own, including images and text.

Digital citizenship

I am responsible for positive digital citizenship. I will treat people with respect and kindness when using technology and online.

- I will be honest and ethical in all digital communications.
- I will be kind and not threaten, insult, gossip about, or tease others in a hurtful way while I am using technology and online.
- I know that failure to properly cite my sources of information is called plagiarism and is a form of cheating.

- I understand that things I share online may be seen by others at school and at home.
- I will not share personal information (either my own or another student's), including where I live, details about family or friends (including names), my age, birthday, home address or telephone number on the internet.
- I will consider whom I am communicating with and think about how they might interpret my words.
- I will use respectful and appropriate language without swearing, name-calling or causing others to feel uncomfortable.
- I will fact-check information before I share it digitally.
- I will not try to trick people into thinking something I wrote was done by someone else.

Personal responsibility and safety

I know that school computers and internet communication tools must be used properly and responsibly.

- I will only log in using my own school-provided username and password.
- If I find content that is not appropriate on the internet, I will notify a teacher or a trusted adult.
- I will take care of my technology from the school as if it belonged to me.
- I will navigate to content on the internet that is directed by my teacher and school staff and is safe for school.
- I understand that my online activity can be viewed by my principal and district administrators.
- I will respect the district network's security measures and only download apps or content I have permission to access.

I understand that using any school technology, networks or devices is a privilege I must earn through responsible use; but we all make mistakes. When I do something with technology that is not in line with this agreement, I will let a trusted adult know and ask them to help me make it right.

If I can't consistently keep my part of this agreement, I understand that privileges may be removed for a time and that I may face additional consequences.

Respect for Technology and Rules

Technology is a powerful tool that helps us learn, create, and connect. To keep our digital environment safe and productive, everyone must follow clear rules for using District technology. These rules protect you, your classmates, and the learning environment.

Violating these expectations may result in the loss of technology access, school disciplinary action, legal consequences, or any combination of these.

Prohibited Use

Users of District technology resources—including computers, networks, software, accounts, and internet access—shall not:

1. **Access or Share Inappropriate Content**
   - Access, view, download, upload, transmit, or distribute content that is obscene, sexually explicit, harmful to minors, or otherwise inappropriate for a school setting.
   - Create or send messages or materials containing vulgar, harassing, threatening, or discriminatory language.
2. **Engage in Cyberbullying or Harassment**

- Use any digital device, platform, or communication method to intimidate, threaten, harass, or demean others.
- Participate in or encourage behaviors that violate the District's anti-bullying and nondiscrimination policies.

3. **Violate Network or System Security**
   - Attempt to bypass internet filters or security protocols, including the use of proxy servers or VPNs.
   - Use another person's login credentials or allow others to use theirs.
   - Attempt to gain unauthorized access to any computer system, network, or file.
   - Introduce or distribute malware, viruses, or other harmful software.
4. **Misuse District Resources**
   - Use District technology for non-educational or personal entertainment purposes unless explicitly permitted by a teacher or administrator.
   - Install unapproved software, applications, or extensions.
   - Engage in online gaming, gambling, or streaming unrelated to instructional activities.
5. **Commit Academic or Intellectual Dishonesty**
   - Plagiarize content from online sources or misuse copyrighted materials.
   - Use generative AI tools in a way that violates classroom rules or academic integrity guidelines.
6. **Disclose Personal or Confidential Information**
   - Share personal information (such as address, phone number, or full name) online without parental and District consent.
   - Disclose or misuse confidential student or staff data.
7. **Use for Unauthorized Financial or Commercial Activity**
   - Engage in buying, selling, fundraising, or advertising without District approval.
   - Incur financial charges through unauthorized use of online services.

Policy Authority

This Acceptable Use Policy is authorized by and consistent with Wentzville R-IV School District Board Policy and Regulation 6320, *Internet Usage*. All students must comply with this policy to retain access to District technology. Violations may result in consequences as outlined in this Acceptable Use Policy and those established under the District's disciplinary procedures. *See, e.g.*, Board Regulation 2610, *Behavioral Expectations* (establishing disciplinary consequences for violations including Technology Misconduct, Cyberbullying, and Academic Dishonesty).

Version and Review Date

Document Version	Approval Date	Next Review Date	Approved By
2025.1	July 17, 2025	July 2027	Board of Education

STAFF ACCEPTABLE USE POLICY

I. Purpose and Authority

The Wentzville R-IV School District ("**District**") provides technology resources to staff to support instruction, enhance learning, and ensure the efficient operation of school programs and services. This Staff Acceptable Use Policy ("**Policy**") sets forth the standards for responsible and professional use of District technology by employees, contractors, and other authorized users.

The purpose of this Policy is to:

1. Define appropriate and inappropriate uses of District technology resources;
2. Promote the secure and ethical use of digital systems and information;
3. Safeguard the confidentiality of student and staff data; and
4. Ensure compliance with applicable Board policies, employment agreements, and local, state, and federal laws.

This Policy is authorized by and consistent with:

1. Board Policy and Regulation 6320 – Internet Usage;
2. Board Policy 4630 – Staff Conduct;
3. Board Policy 4650 – Communication with Students by Electronic Means;
4. Board Policy 3106 – Fraud Prevention; and
5. Board Policy and Regulation 5710 – Data Governance.

Nothing in this Policy shall be construed to supersede the rights and responsibilities established under any applicable collective bargaining agreement.

II. Scope and Applicability

This Policy applies to all employees of the District, including full-time and part-time staff, administrators, substitute personnel, contractors, interns, and volunteers who access or use District technology resources.

District technology resources covered by this Policy include, but are not limited to:

1. District-owned computers, tablets, and other digital devices;
2. District email systems and communication platforms;
3. Access to the District's network, Wi-Fi, and internet;
4. Cloud-based platforms and services provided or authorized by the District (e.g., Google Workspace, learning management systems);
5. Any software, applications, or digital content hosted, licensed, or supported by the District.

This Policy governs use of District technology resources both on and off District property, during and outside of work hours, to the extent that such use involves District equipment, services, accounts, or student/staff data.

III. Acceptable and Unacceptable Use

A. Acceptable Use

District technology resources are provided to support the educational mission of the District and to enable staff to perform their professional responsibilities effectively. Acceptable use includes:

1. Accessing and using District systems for instructional, administrative, or job-related purposes;
2. Communicating professionally with students, families, colleagues, and community members through District-provided platforms;
3. Accessing approved educational resources, software, and communication tools to support learning and District operations;
4. Maintaining the confidentiality and integrity of student and staff data, consistent with applicable law and Board policy;
5. Supervising student technology use in accordance with the District's instructional goals and legal obligations.
6. Incidental personal use is permitted if it does not interfere with job responsibilities, violate District policy, or compromise system integrity or security.

B. Unacceptable Use

The following uses of District technology resources are strictly prohibited. This list is not exhaustive and includes, but is not limited to:

- Accessing, creating, or distributing obscene, offensive, or otherwise inappropriate material;
- Engaging in harassment, bullying, or discriminatory conduct through digital platforms;
- Communicating with students in a manner that violates Board Policy 4650;
- Accessing or attempting to access systems, data, or accounts without proper authorization;
- Circumventing or attempting to bypass District security or content filtering measures;
- Using another individual's login credentials or sharing personal access credentials;
- Downloading, installing, or using unauthorized software or applications;
- Engaging in any activity that may harm the District's network or information systems, including the introduction of malware or viruses;
- Using District technology for personal commercial gain, fundraising, or other non-District business;
- Using District technology for purposes other than District business.
  - As required by Board Policy 4630, employees must utilize District technology solely for school district business. Personal, commercial, political, or recreational use that is not incidental and explicitly authorized is prohibited;
- Engaging in political advocacy using District resources.
  - Employees may not use District technology, email, networks, devices, or staff time to advocate, support, or oppose any ballot measure or candidate for public office. This restriction is required by § 115.646, RSMo., and applies to all forms of District-funded communications or activity, unless specifically permitted by law (*e.g.*, informational press releases). A purposeful violation of this statute is a Class Four election offense and may result in both disciplinary and legal consequences;
- Violating copyright, licensing, or intellectual property laws;
- Storing personal or non-District files using District systems;
- Failing to comply with data privacy requirements under FERPA, HIPAA, or other applicable laws.

Employees who are uncertain whether a specific use is permissible should consult their supervisor or the Technology Department before proceeding.

IV. Data Security and Confidentiality

A. Protection of Student and Staff Information

All employees are expected to maintain the confidentiality, integrity, and lawful use of student, staff, and District data. Staff must comply with all applicable privacy and data protection laws and Board policies, including:

- FERPA;
- HIPAA, as applicable;
- CIPA;
- Board Policy and Regulation 5710 – Data Governance.

District data must only be accessed, used, and shared for legitimate educational or operational purposes. Unauthorized access, use, disclosure, or distribution of confidential information—whether intentional or accidental—may result in disciplinary action and legal liability.

B. Secure Use of District Systems

Employees must take reasonable and proactive measures to ensure the security of District systems and data, including:

1. Using strong, unique passwords and safeguarding login credentials;
2. Locking devices when left unattended;
3. Accessing only data necessary to fulfill assigned job responsibilities;
4. Reporting suspected data breaches, account compromises, or other security incidents immediately to the Technology Department;
5. Avoiding the use of unauthorized cloud storage platforms, applications, or data-sharing tools;
6. Using only District-approved systems to transmit, store, or access confidential information.

C. Restrictions on Personal Devices and Storage

Employees are prohibited from downloading, storing, or transmitting District data—especially confidential or personally identifiable information—on personal devices, removable drives, or non-District cloud services, unless specifically authorized by the

District and secured in accordance with applicable data governance protocols. All such uses must meet District encryption and access control standards.

V. Monitoring and Privacy

A. Monitoring of Use

The District reserves the right to monitor, access, and review all use of its technology resources to ensure compliance with this policy, to maintain system integrity and security, and to fulfill its legal obligations. This includes monitoring:

1. Internet usage and browsing activity;
2. District email and messaging platforms;
3. Files stored on or transmitted through District systems;
4. Device activity on District-owned hardware.

Monitoring may occur at any time, with or without prior notice, and may be conducted by authorized District administrators or technology staff.

B. No Expectation of Privacy

Employees should have no expectation of privacy when using District technology resources, including while using District-owned devices or accessing District accounts from personal or off-site locations. All data created, transmitted, received, or stored using District systems is the property of the District and may be subject to disclosure under law or policy.

C. Reporting and Cooperation

Employees are required to promptly report suspected violations of this policy, data breaches, or unauthorized access to technology systems. Failure to report known or suspected misuse may itself be treated as a policy violation. Staff are expected to cooperate with any authorized investigation into misuse of District technology.

VI. Enforcement and Disciplinary Action

A. Consequences for Policy Violations

Violations of this policy may result in disciplinary action, up to and including revocation of technology privileges, suspension, termination of employment, or legal referral, depending on

the nature and severity of the offense. Technology misuse may also result in civil or criminal liability where permitted or required by law.

Disciplinary decisions will consider the context of the violation, the employee's role, intent, prior conduct, and the impact on students, staff, and District operations.

B. Governing Policies and Legal Standards

Enforcement of this policy shall be carried out in accordance with applicable Board policies, administrative regulations, and employment agreements, including:

1. Board Policy 4630 – Staff Conduct;
2. Board Policy 4650 – Communication with Students by Electronic Means;
3. Board Policy 3106 – Fraud Prevention;
4. Board Policy and Regulation 6320 – Internet Usage;
5. Board Policy and Regulation 5710 – Data Governance;
6. Any applicable provisions of collective bargaining agreements.

Where applicable, violations may also implicate legal standards under FERPA, HIPAA, CIPA, and Missouri Revised Statutes, including but not limited to § 115.646.

C. Due Process and Representation

Employees subject to disciplinary action under this policy will be afforded the due process protections provided by Board policy and regulation. Where applicable, additional procedures related to representation, notification, and documentation may be informed by provisions in collective bargaining agreements.

VII. Acknowledgment and Agreement

As a condition of employment and access to District technology resources, all staff are required to acknowledge and agree to the terms of this policy.

A. Staff Certification

All employees must certify annually that they have read, understand, and agree to comply with the Staff Acceptable Use Policy. Certification may occur electronically or in writing as determined by the District.

B. Record Retention

Acknowledgments will be maintained by the District and may be retained in the employee's personnel file or within the District's electronic compliance system, as applicable.

VIII. Definitions

A. CIPA

The Children's Internet Protection Act, 47 U.S.C. § 254(h)(5); a federal law requiring K–12 schools to implement internet safety policies and technology filters to protect minors from harmful online content.

B. FERPA

The Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g; a federal law protecting the privacy of student education records and governing the disclosure of personally identifiable student information.

C. HIPAA

The Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d et seq.; a federal law that protects the confidentiality of individually identifiable health information, applicable to school health staff under specific conditions.

D. District Technology Resources

Includes all hardware, software, accounts, systems, internet access, cloud services, digital platforms, and communication tools provided, licensed, or supported by the District.

E. Confidential Information

Any information that is not public and is protected by law, regulation, or District policy, including but not limited to student records, staff records, medical data, disciplinary records, and login credentials.

F. Staff

Any full-time or part-time employee, administrator, substitute, contractor, intern, or volunteer who accesses or uses District technology systems.

G. Monitoring

The authorized review, logging, or inspection of digital activity, files, or communications to ensure compliance with District policy, system security, or legal requirements.

IX. Related Policies and References

This Policy is supported by and must be interpreted in conjunction with the following Board policies and applicable laws:

A. Board Policies and Regulations

1. Board Policy and Regulation 6320 – Internet Usage
2. Board Policy and Regulation 5710 – Data Governance
3. Board Policy 4650 – Communication with Students by Electronic Means
4. Board Policy 4630 – Staff Conduct
5. Board Policy 3106 – Fraud Prevention

B. Federal and State Laws

1. FERPA
2. HIPAA
3. CIPA
4. § 115.646, RSMo – Prohibited Use of Public Funds for Political Advocacy

Employees are expected to familiarize themselves with these policies and laws as they pertain to the responsible use of District technology.

X. Questions and Support

Employees are encouraged to seek clarification when unsure about the appropriate use of District technology or their obligations under this policy.

For questions, reporting concerns, or requesting technical assistance, staff should contact:

Technology Department
(636) 332-3751 ext. 22330

For questions related to employee conduct, professional expectations, or disciplinary matters, staff may also contact:

Human Resources Department
(636) 327-3800 ext. 20351

In matters involving potential policy violations, employees may also contact their building administrator or immediate supervisor.

XI. Version and Review Date

Document Version	Approval Date	Next Review Date	Approved By
2025.1	July 17, 2025	July 2027	Board of Education

This policy will be reviewed and updated as necessary to reflect changes in law, technology standards, District policy, or professional expectations.

1. Acknowledgment Statement

I acknowledge that I have read and understand the Wentzville R-IV School District Staff Acceptable Use Policy. I agree to comply with its terms and with all related Board policies, administrative regulations, and legal requirements. I understand that misuse of District technology resources may result in disciplinary action, including loss of access privileges, termination of employment, and legal consequences. I further understand that I have no expectation of privacy when using District systems and that my use may be monitored in accordance with this policy.

_____

Employee Name (Printed)

_____

Employee Signature

_____

Date