

Trigg County Schools Staff Responsible Use Policy

I. Introduction

All employees of Trigg County Schools are expected to use the district's technology resources responsibly, ethically, and in compliance with applicable laws, regulations, and board policies. This policy outlines appropriate practices to ensure staff uphold professional standards while maintaining the privacy and safety of students, colleagues, and district data.

II. Legal and Ethical Compliance

Trigg County Schools staff must comply with all applicable federal, state, and local regulations including but not limited to:

- Family Educational Rights and Privacy Act (FERPA)
- Children's Internet Protection Act (CIPA)
- Individuals with Disabilities Education Act (IDEA)
- Children's Online Privacy Protection Act (COPPA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Kentucky law (e.g., SB 181, KRS 61.931)
- District Board Policy

Violations may result in disciplinary action up to and including termination or legal action. The district will cooperate fully with authorities as required.

III. Acceptable Use of Technology

District-provided devices, network, email, and internet access are provided to enhance education and job performance. This access is a privilege—not a right.

A. Permitted Use

- Use district systems primarily for professional, educational, and administrative purposes.
- Model and teach positive digital citizenship.
- Use professional language in communications and content.

B. Prohibited Use

The following uses are strictly prohibited:

1. Unauthorized personal use that interferes with job responsibilities.
2. Sharing or accessing confidential student or employee information without authorization.
3. Distributing or downloading copyrighted materials without permission.
4. Engaging in cyberbullying, hate speech, sexually explicit, or violent content.
5. Using district systems for personal financial gain, commercial activity, or political endorsements.
6. Bypassing security measures, including the use of proxy servers or unauthorized software.
7. Tampering with district hardware, software, or network infrastructure.
8. Granting access to district systems or data to unauthorized persons.
9. Using “hacking” tools or engaging in activities aimed at breaching security.
10. Using personal social media to post content that disrupts school operations or compromises safety.

IV. Artificial Intelligence (AI) Use

Employees may use generative AI (GenAI) tools to enhance productivity and support instruction, provided that:

- AI complements, not replaces, professional judgment.
- Teachers maintain transparency in AI-assisted work.
- AI is used ethically, without introducing bias or inequity.
- Credit is given where due; plagiarism is strictly prohibited.
- Data privacy and FERPA-compliance are maintained.

V. Digital Citizenship and Professional Responsibility

All staff must:

- Model appropriate digital behavior and online etiquette.
- Teach and reinforce digital citizenship in classroom settings.
- Actively protect student data and district systems.

- Use only approved district systems to transfer student data.
- Maintain professional conduct and communication at all times.
- Only utilize Board approved communication tools to communicate with students (ex ParentSquare, Gmail) SB 181

VI. Security and Privacy

A. Passwords and Accounts

- Never share passwords or access credentials.
- Log out of devices and systems when unattended.
- Use only district-approved platforms and applications.

B. Device and Network Use

- Report any stolen or lost devices immediately.
- Do not install unauthorized software or hardware.
- Be cautious of phishing emails, malware, and other threats.
- Use devices responsibly to prevent damage or misuse.

C. Personal Devices

- Personal devices are not supported by district technology staff.
- The district is not responsible for personal device loss, theft, or damage.
- Never use personal devices to record or photograph students/staff without written consent.

VII. Copyright and Intellectual Property

- Adhere to all copyright laws and licensing agreements.
- Do not download, distribute, or share illegally obtained materials.
- Respect intellectual property rights of others in all work.

VIII. Monitoring, Auditing, and Limited Personal Use

The district reserves the right to monitor all technology use. There is no expectation of privacy when using district systems. Limited personal use may be permitted, provided it:

- Does not interfere with work duties.
- Does not incur additional cost to the district.
- Does not violate this policy or any law.

IX. Consequences

Violations of this policy may result in:

- Revoked access to technology resources.
- Disciplinary action, up to and including termination.
- Criminal or civil liability, depending on the nature of the violation.

All incidents must be reported immediately to a supervisor or the Help Desk. Suspected illegal activity should also be reported to law enforcement.

X. Disclaimer

Trigg County Schools makes no guarantees regarding service quality or data security on its network. The district is not responsible for data loss, inaccuracies, or damages resulting from the use of its technology resources.

Acknowledgment

I have read and understand the Trigg County Schools Staff Responsible Use Policy. I agree to follow the guidelines and will act in a responsible, ethical, and legal manner when using district technology.

Employee Name: _____

Signature: _____

Date: _____