

Riverview Community School District

Acceptable Technology Use Agreement



I. Purpose

Riverview Community School District provides information and technology resources, including district-assigned devices, district-managed accounts, networks, and internet access, to support instruction, operations, and professional responsibilities.

This agreement establishes expectations for the responsible, ethical, and secure use of all district-provided technology resources by staff in a manner consistent with district policies, professional standards, and applicable laws and regulations.

II. Scope

This policy applies to all staff including all employees, contractors, and authorized users acting on behalf of the district who use:

- District-owned or district-assigned devices
- District networks, including wired and wireless systems
- District-managed accounts (including Google, Microsoft, and approved third-party applications)
- Internet, email, and cloud-based resources accessed through district systems

III. Responsibilities for Devices

Staff are responsible for:

- Using district-issued devices primarily for educational, instructional, and professional purposes
- Exercising reasonable care in the use, handling, and storage of devices
- Maintaining the security of devices and not leaving them unattended in unsecured locations
- Transporting devices in a safe and responsible manner
- Using only devices and accounts assigned to them, unless otherwise authorized
- Promptly reporting damage, loss, theft, or technical issues to the Technology Department

Staff may not:

- Remove, alter, or obscure district asset tags or serial numbers
- Modify device hardware or internal components without authorization
- Install or use operating systems, firmware, or software not approved or supported by the district
- Attempt to bypass, disable, or interfere with district security, filtering, monitoring, or device management controls

IV. Loss, Theft, and Damage

- Loss, theft or damage of district-issued devices may result in a replacement charge
- Loaner devices are subject to the same expectations

V. Network and Internet Use

Staff are expected to:

- Use district networks, internet access, and online resources in a professional, ethical, and responsible manner
- Follow district policies, administrative guidelines, and professional conduct standards while using technology
- Use district networks primarily to support instructional, operational, and professional responsibilities
- Protect the confidentiality of student and staff information while using digital systems
- Comply with applicable local, state, and federal laws and regulations

Staff may not:

- Access, create, transmit, or display content that is unlawful, offensive, obscene, or inappropriate for a school environment
- Engage in harassment, bullying, intimidation, or discriminatory conduct through district technology resources
- Share personally identifiable information, confidential data, or protected student information without proper authorization
- Access, use, or share another individual's account, credentials, or passwords
- Intentionally access, alter, damage, or disrupt district systems, networks, or data
- Violate copyright, licensing, or intellectual property laws
- Use district technology resources for personal commercial activities, fraud, or financial gain without prior authorization

VI. Monitoring and Privacy

- The District reserves the right to monitor, review, access, and inspect activity conducted on district-owned devices, networks, and district-managed accounts, as permitted by law.
- Staff should not expect privacy in files, communications, or data created, accessed, transmitted, or stored on district systems or devices.
- District network storage, email, and cloud-based systems are provided for professional use and may be reviewed during system maintenance, security, compliance, or administrative investigation.
- Monitoring activities will be conducted in a manner consistent with applicable laws, district policies, and collective bargaining agreements.

VII. Digital Citizenship Expectations

Staff are expected to model and demonstrate responsible digital citizenship by:

- Engaging in respectful, professional, and ethical online interactions
- Protecting personal, student, and staff account information and credentials
- Communicating appropriately and in accordance with district standards and professional expectations
- Safeguarding confidential and sensitive information
- Respecting copyright, licensing agreements, and intellectual property rights
- Acting with integrity, professionalism, and sound judgment in all digital interactions

VIII. Publishing and Student Work

Staff are responsible for ensuring that the publication or sharing of student work, images, or information complies with district policy and applicable laws.

Staff must:

- Publish or share student work only through district-approved platforms or channels
- Obtain and honor parent or guardian consent in accordance with district enrollment forms and photo/media release preferences
- Ensure that student images used to highlight school activities do not include identifying information unless permitted
- Publish student names or identifying information only for legitimate educational or school-related purposes and in compliance with district guidelines
- Protect student privacy when sharing instructional materials, projects, or examples

IX. Accounts and Applications

- Staff are issued district-managed accounts, including Google, Microsoft, and other approved platforms, for instructional and professional use.
- Staff may use district-approved applications and services, including artificial intelligence (AI)-enabled tools, when such use aligns with instructional goals, operational needs, and district guidance.
- Staff are responsible for ensuring that any applications or tools used with students are approved by the district and comply with student data privacy, security, and accessibility requirements.
- The use of all accounts and applications is subject to district policies, filtering, monitoring, and applicable local, state, and federal laws and regulations.
- Staff may not create, require, or direct students to use non-approved accounts or applications without prior authorization.

X. Artificial Intelligence

Educational and Professional Use of AI

Riverview Community School District recognizes that artificial intelligence (AI) tools may support instructional planning, learning experiences, creativity, and operational efficiency when used responsibly and ethically.

Staff may use AI tools to support professional and instructional work when using such:

- Aligns with district policies and instructional goals
- Maintains appropriate human oversight and professional judgment
- Protects student privacy and confidentiality
- Comply with applicable laws and district data governance requirements

Instructional Use with Students

- Clearly communicating expectations, limitations, and permitted uses to students
- Ensuring AI use aligns with learning objectives and grade-level appropriateness
- Promoting academic integrity and transparency
- Ensuring that AI tools do not replace independent student thinking unless explicitly intended as part of instruction

Prohibited Uses of AI by Staff

- Representing AI-generated or AI-assisted content as wholly original professional work when disclosure is required
- Use AI tools to replace professional judgment in grading, evaluation, or disciplinary decision-making
- Use AI to generate or modify student work, assessments, or evaluations in a manner that misrepresents student performance
- Use AI tools to bypass curriculum standards, assessment integrity, or district safeguards
- Enter personally identifiable student or staff information into AI tools that are not approved by the district

XI. Violations and Consequences

Violation of this policy may result in disciplinary action in accordance with school policies and procedures.

XII. Legal and Regulatory Compliance

Riverview Community School District complies with applicable federal and state laws and regulations, including the Children’s Internet Protection Act (CIPA) and the Family Educational Rights and Privacy Act (FERPA), through appropriate filtering, monitoring, and data protection measures.

XIII. Liability

Riverview Community School District is not responsible for incidental or unintended issues arising from the use of district-provided technology resources, including device malfunction, service interruptions, or data loss that may occur despite reasonable safeguards. The district is also not responsible for the interception of data during technology use, provided that applicable federal and state data privacy and security laws are followed. Staff are expected to use district technology resources responsibly and in accordance with this policy and all district applicable guidelines. Staff are responsible for taking reasonable precautions to protect district equipment, accounts, and data.

XIV. Agreement and Acknowledgement

By signing below, the staff members acknowledge that they have read, understand, and agree to comply with the terms and conditions of this Staff Acceptable Technology Use Agreement, as well as all applicable district policies and administrative guidelines.

Employee's Signature: _____ Date: _____