Rocklin Unified School District Employee Authorized Network, Internet Usage, and Email Privacy Agreement

---

Please read this document carefully before signing:

A. General Provisions

Employees are required to review and sign this agreement **annually** to reaffirm their understanding and compliance with the policies outlined herein. Upon employment, all individuals permitted to use the Rocklin Unified School District (RUSD) network, online services, and computing resources are required to sign this agreement and abide by Board Policies 4040 (Employee Use of Technology), as well as corresponding regulations, the Children's Internet Protection Act (CIPA), the Health Insurance Portability and Accountability Act (HIPAA), state and federal laws, and all policies within.

Upon employment, each individual permitted to use the District's computing resources becomes responsible for protecting the resources and data they control or access. Computing resources are provided to support instructional and administrative objectives and academic research. Employees shall be responsible for appropriate technology use and shall utilize District resources solely for employment-related purposes.

B. Employee Use Guidelines

1. Respect the rights of other District network users. Knowingly accessing or sharing data files or e-mail messages without permission is prohibited.
2. Be professional and appropriate in all communications.
3. Adhere to legal, ethical, and academic integrity standards when using the network.
4. The District's computer network must not be used to send, download, store, or create materials that contain defamatory, obscene, pornographic, profane, sexually oriented, threatening, racially offensive, discriminatory, or illegal content.
5. The District's computers, network equipment, programs, and supplies must be used solely for work-related purposes and not for personal financial gain.
6. Personally owned devices must not be connected to the network without approval from the Information Technology Department.

C. Use of Artificial Intelligence (AI)

1. Employees must ensure that AI tools used in the classroom or for work have been vetted and approved by the District.
2. The District may require parental consent before offering AI services to students.
3. AI tools should be evaluated for data privacy, equity, bias mitigation, and accuracy before implementation.

4. Teachers must clearly communicate how and when students can use AI for assignments and must monitor student use to ensure compliance with District policies.
5. Employees must not share confidential or personally identifiable information (PII) with AI systems.
6. Employees should follow the AI guidance outlined in the District's "Empowering RUSD with Responsible AI Use" document.
7. AI-generated content should not replace teacher-led instruction, assessments, or student originality in academic work.

D. Social Media Usage

1. Employees must exercise caution when interacting with students on social media and must not engage in private, direct messaging unless required for instructional purposes and approved by the administration.
2. Employees must adhere to professional conduct standards when posting content that could be associated with RUSD.
3. Employees must not share confidential student or staff information on social media platforms.
4. Any social media account representing the District or a school must be authorized and monitored by District personnel.
5. Employees should not post content that could compromise student privacy, safety, or the reputation of the District.
6. Employees should use District-approved communication platforms when engaging with students for educational purposes.

E. Student Data Privacy & Security

1. Employees must ensure that student data is handled in compliance with federal and state regulations, including FERPA and CIPA.
2. Employees must only use District-approved platforms for storing or sharing student information.
3. Employees should never enter student PII into unapproved AI tools or external applications.
4. Student assessment data should be handled in accordance with BP 6162.5 to ensure data integrity and accuracy.
5. Employees must report any suspected data breach or unauthorized access immediately to the Information Technology Department.

F. Multi-Factor Authentication & Password Management

1. Employees must use **id.rocklinusd.org** for managing their District passwords.
2. Multi-factor authentication (MFA) must be enabled on all applicable District accounts.
3. Passwords should be strong, unique, and changed periodically to maintain security.
4. Employees must not share passwords or store them in unsecured locations.

5. The use of password managers approved by the District is encouraged for enhanced security.

G. User Responsibilities

1. Employees must assist in maintaining network security by not opening suspicious emails or attempting to bypass security measures.
2. Employees must only access authorized computers, applications, and files.
3. Confidential information, including student data, should not be shared via email unless necessary and labeled appropriately.
4. Passwords must be kept confidential and changed periodically to maintain security.
5. The District monitors internet usage, and violations may result in loss of privileges or disciplinary action.
6. Employees should report cybersecurity concerns, including phishing attempts, to the IT Department immediately.
7. Employees must not store sensitive District information on personal devices.

H. Remote Access

1. Employees granted remote access must ensure secure connections and comply with District security policies.
2. Remote access is monitored, and employees are responsible for maintaining security standards comparable to on-campus access.

I. Acknowledgment and Agreement

By signing this document, I acknowledge that I have read and understand the Rocklin Unified School District Employee Authorized Network, Internet Usage, and Email Privacy Agreement. I understand that violations of these policies may result in disciplinary action or legal consequences.