Technology Acceptable Use Policy - FL

Table of Contents

Policy Effective Date July 1, 2026

Introduction: Welcome to the Juab School District Acceptable Use Agreement, designed to ensure a safe and productive digital environment for all users. We're here to encourage responsible and educational use of technology resources. Please read and understand these guidelines, as they outline how to maintain a respectful and secure digital atmosphere.

Teaching digital well-being doesn't mean providing students with a list of "don'ts." It's about the do's – modeling and practicing skills that help young people become thoughtful, empathetic digital citizens who know how to use technology to learn and solve problems in their digital and physical communities.

The digital citizenship competencies, developed by the ISTE-led DigCit Coalition in conjunction with coalition partners, shift the conversation from don'ts to do's:

Balanced	Students participate in a healthy variety of online activities and know how to prioritize their time between virtual and physical activities.
Informed	Students evaluate the accuracy, perspective, and validity of digital media, and have developed critical skills for curating information from digital sources.

	Inclusive	Students are open to hearing and recognizing multiple viewpoints and engaging with others online with respect and empathy.
	Engaged	Students use technology and digital channels to solve problems and be a force for good in their families and communities.
	Alert	Students are aware of their digital actions and know how to be safe and create safe spaces for others online.

Acceptable Uses of the Juab School District Networks

Educational Focus	Use technology resources for educational and professional purposes aligned with learning objectives. Maintain appropriate digital behavior when collaborating, communicating, or publishing online.
Permission & Acknowledgment	Students under age 18 must have a signed acknowledgment from a parent or guardian on file before independent use of district-provided devices or online services.
Reasonable Precautions	Protect district data and systems by following security practices such as password protection and multi-factor authentication when available.
Personal Use	Staff may use the internet for limited personal use during duty-free time.
Seek Guidance	Report security or content concerns promptly to Administration.

Unacceptable Use

Protect Personal Information	Never share personal information on the internet. This includes names, addresses, phone numbers, and photos. Avoid meeting people in person who you've only met online.
Unauthorized Access	Users shall not disable or attempt to bypass district security controls, including firewalls, endpoint protection, and filtering systems.
Inappropriate Content	Avoid accessing, sharing, or creating offensive, sexually explicit, or otherwise inappropriate content. This includes materials that are illegal or defamatory.
Respect Copyright	Do not download, upload, or distribute files, software, or materials in violation of copyright laws.
Plagiarism	Do not plagiarize. Always give proper credit for sources and information used.

Cyberbullying & Harassment	Do not engage in cyberbullying, harassment, or threats of violence as defined under Utah's SafeUT and anti-bullying statutes. (Utah Code §53G-9-601)
No Harmful Messages	Avoid sending messages that are offensive, discriminatory, or encourage illegal activities. Do not send messages related to dangerous devices or weaponry.
Illegal Activities	Do not engage in any criminal activities online that violate any local, state and federal laws.
Interference	Do not disrupt computer systems, equipment, or network performance. This includes intentionally accessing, transmitting, or downloading harmful files or programs.
Hacking & Unauthorized Access	Do not engage in hacking activities or attempt to access private information. Attempts to circumvent firewalls and filters are prohibited; this includes VPNs.
Commercial Use	Do not use the network for commercial purposes, personal advertising, or fundraising for non-government-related activities.
Physical Misuse	Do not cause damage or tamper with district devices or technology infrastructure, whether intentional or unintentional.

User Responsibilities

- Users must read, understand, and follow these guidelines.
- Exercise judgment in interpreting these guidelines.
- Seek clarification from a Juab School District administrator when in doubt.
- Do not go beyond authorized access.
- Report any security problems promptly.

Administrator Responsibilities

- Administrators must ensure understanding and compliance with this policy.
- Report any misuse of the system to Juab School District officials.
- Review monitoring tools to determine if student accounts are in compliance when misuse is suspected.

Educator Responsibilities

- Educators must teach students about safe internet use.
- Monitor students' online activities and intervene if misuse is observed.
- Report student misuse to administrators or Juab School District officials.

Student Responsibilities

- Learn safe and responsible internet use.
- Abide by the Acceptable Use Agreement.
- Understand that some internet content may be inappropriate.
- Use district resources responsibly.
- Report other students' misuse to teachers or administrators directly or via SafeUT.

System Monitoring and Limited Privacy

- Students and Staff are granted access to district technology for educational purposes and should not expect personal privacy for files, emails, or other content on district-provided services or equipment. All activity and communications on the district network are subject to review.

- To protect students/staff and maintain system integrity, the District may monitor online activities and access, review, copy, or store electronic communications or files as necessary to enforce policy and ensure a safe educational environment.

Artificial Intelligence (AI)

- All students and staff must use Artificial Intelligence (AI) tools responsibly and in alignment with the Utah P-12 AI Framework. AI may only be used for educational or administrative purposes.
- Users must not use AI to create harmful, misleading, or inappropriate content, including fabricated data, impersonation, or deepfakes.

Security Cameras/Surveillance

- Security cameras are placed throughout district property to protect students, staff, and assets.
- Posted notice will indicate areas under surveillance.
- Video and audio recordings are retained only as long as necessary under district records policy.
- Access to recordings is limited to authorized Administration, School Resource Officers (SROs), or law enforcement when legally required.
- Surveillance footage may only be used for safety, security, or disciplinary purposes in accordance with Utah Code §53G-8-802.
- Classroom Cameras exceptions and specifications can be found here.

Data Privacy and Legal Compliance

- Juab School District complies with the Family Educational Rights and Privacy Act (FERPA), the Utah Student Data Protection Act (§53E-9), the Children's Internet Protection Act (CIPA), and the Children's Online Privacy Protection Act (COPPA).
- Personally identifiable information (PII) will be collected, used, and shared only as permitted by law and district data governance policies. Internet filtering and monitoring are implemented to comply with CIPA and ensure student safety.
- Students under 13 may not provide personal information to online services without verified parental consent.

Passwords

- Users must safeguard their credentials and are responsible for all activity under their accounts.

Password requirements:

- Minimum of 12 characters
- At least one number and one special character
- Not easily guessed
- Staff are encouraged to use two-factor authentication (2FA) whenever possible.

Accessibility and Equity

- Juab School District ensures that technology resources and digital content are accessible to all users, consistent with Section 504 of the Rehabilitation Act and the Americans with Disabilities Act (ADA).

Violations

- Violations of this AUP may result in disciplinary action by district administrators, including suspension of technology access, confiscation of devices, or other measures consistent with district policy and Utah Administrative Code R277-495.
- Users accused of violating this policy will receive notice and an opportunity to respond. Disciplinary action will be proportionate to the violation.

Disclaimers

Juab School District makes no warranties, expressed or implied, regarding technology services or resources. The District is not responsible for damages, data loss, or financial obligations resulting from use of district technology. While technical and administrative safeguards are employed, no filtering or monitoring system is foolproof. All provisions of this AUP are subordinate to local, state, and federal law.

Policy Review and Contact

This policy will be reviewed annually by Juab School District Administration to reflect updates in law and technology practice. Questions about this policy should be directed to the Administration.

References

ISTE Digital Citizenship Framework
Utah P-12 Artificial Intelligence Framework
Family Educational Rights and Privacy Act (FERPA)
Utah Student Data Protection Act (§53E-9)
Children's Internet Protection Act (CIPA)
Children's Online Privacy Protection Act (COPPA)
Utah Code §53G-8-802 – Use of Video Surveillance
Utah Code §53G-9-601 – Bullying and Cyberbullying
Utah Administrative Code R277-495 – Required Policies for Electronic Devices
Section 504 of the Rehabilitation Act (29 U.S.C. § 794)
Americans with Disabilities Act (ADA, 42 U.S.C. § 12101)