



Communications Policy

Policy Series 3000: General Board

Policy No. 7600 P1

Digital Communication

These procedures apply to all **Cache County School District (CCSD)** employees. This section outlines the standards for digital engagement to ensure professional, secure, and effective communication with our community.

All employees must comply with the **Utah Educator Professional Standards**, specifically avoiding private interactions with students via digital platforms (Utah Code R277-515-2). Whether using district-provided tools or personal devices, professional ethics and CCSD policies always apply.

Legal Compliance: All users must follow data privacy and ADA laws and policies. (CCSD Policy 6900 and Utah Code §63A-16-209)

Copyright and Citations: Do not post copyrighted material without written consent from the owner. All shared content must include a standard citation and a direct link (URL) to the original creator.

External Links: Links to unofficial, off-site CCSD-related pages are prohibited unless they directly support the district's operations or academic mission, comply with all federal, state, and district regulations, and have been approved by district administration. Exercise caution when sourcing information or images from external websites.

Prohibited Content: Digital communication—including email, social media, and websites—may not be used for commercial advertising, political lobbying, or personal financial gain. Any outside shared content must follow the distribution of materials procedures and process.

Public Records and Archiving (GRAMA): In Utah, digital communications (including texts and social media posts) made in an official capacity are subject to the Government Records Access and Management Act (GRAMA). All digital communications, including social media posts and SMS sent via district platforms, are considered public records. Employees should have no expectation of privacy when using district-approved communication tools.

Artificial Intelligence (AI): Only district-approved AI platforms should be used. When using AI tools to assist in content creation, employees must review all output for accuracy and tone. **Never** input personally identifiable information of either employees or students (names, ID numbers, etc.) or confidential data into unauthorized third-party AI platforms.

Accessibility: All images posted to websites must include descriptive 'Alt-Text.' All videos containing spoken word must include accurate closed captioning to ensure accessibility for the hearing impaired.

Directory Information:

- **Public Staff Data:** Official sites may list employee names, CCSD emails, official photos, and CCSD phone numbers.
- **Privacy:** Do not share personal contact information for staff or non-school employees.
 - **Exceptions:** Contact details for volunteers in official roles (e.g., School Boards, PTA/PTSO, Booster Clubs, or Community Councils) may be shared.
- **Opt-Out:** Employees must contact the Human Resources Department to opt out of directory listings.

Email and Newsletters

Email is the primary record-keeping and formal communication tool for CCSD.

- **Official Accounts:** Employees must use district-issued email addresses for all professional correspondence.
- **Mass Email Lists:** Any group email list must be approved and coordinated by building administration and follow the process outlined by the technology department. Group email lists are for work-related purposes. Advertising products or services is not allowed via group emails and should be distributed only in accordance with the distribution of materials policy.
- **Newsletters:** School and department newsletters should be distributed through district-approved platforms to ensure brand consistency, accessibility compliance (ADA), and data privacy laws and procedures.
- **Content:** Communications should be concise, professional, and focused on school-related business. Avoid using "Reply All" unless essential.

SMS (Short Message Service, Including Texting) and MMS (Multimedia Messaging Service)

While convenient, text messaging should be used judiciously and primarily for logistical or urgent updates.

- **Mass Messaging:** Schools should use only district-integrated platforms (e.g., ParentSquare) to send SMS/MMS alerts and follow the communications office's current processes and best practices.

- **Direct Messaging:** One-on-one texting with students is prohibited. If texting a parent is necessary, employees should use a district-approved application that archives the conversation. (e.g., ParentSquare)
- **Media:** All MMS content must adhere to FERPA regulations. Students may only appear in multimedia if a parent or legal guardian has signed a media release, and all such files must be transmitted via official district channels.

Content Creation Platforms (YouTube, Instagram, Facebook, etc.)

- **Management:** Official school, department, or program accounts must be approved by the school administration and the CCSD communications department. Accounts must be managed by a full-time employee and accessible to the communications office. All official Instagram and Facebook accounts must be approved and housed under the district's Meta Business account.
- **Monitoring:** Administrators are responsible for regularly auditing school accounts to ensure content is current, professional, and compliant with CCSD policy and current data privacy laws.
- **Public Access:** Information intended for the general public must be hosted on platforms that do not require a private "follow" or "friend" request for basic access.
- **Public Comment:** Official social media accounts that allow public comments must post or link to the district's standard 'Terms of Use.' Comments may only be removed if they violate specific, content-neutral rules (e.g., profanity, hate speech, or spam), in consultation with the communications department.
- **Account Information:** Accounts must be approved by and coordinated with the building administrator and the CCSD communications office. Accounts must follow CCSD's current best practices.
 - Account managers are responsible for all content posted to the account.
 - Upon resignation or transfer, account managers must ensure all administrative credentials are transferred to the building principal and the communications department.
 - Personal email addresses may never be used as recovery methods for official accounts.

CCSD Websites

- Official school, department, or program webpages must be hosted on the CCSD main website with the current host provider and must follow CCSD brand identity. (e.g., FinalSite)
- All official sites must comply with ADA requirements.

- The communication office acts as the district’s webmaster. Schools, departments, and programs may have a trained web editor to update pages under the direction of the communications department.
- Classroom websites are allowed with the building administration's approval. They must be housed under the current contracted platforms and follow policy and procedures. (e.g., Google Sites, Canvas)

Emergency Communications

In the event of an emergency or crisis, information must be centralized to be timely and accurate, and to prevent the spread of misinformation.

- **Priority:** Emergency alerts take precedence over all other communications.
- **Standardized Messaging:** Only authorized personnel, the superintendent, PIO, or designee, should initiate district-wide emergency broadcasts via SMS, email, websites, social media, etc.
- **Protocol:** Follow the established Standard Response Protocol (SRP) when drafting emergency alerts to ensure clear, actionable instructions.
 - Building emergency communications must be coordinated and approved by the student services and/or communications department.

References

Cache County School District. (n.d.). *Policy 6900: Information technology resources and security*. <https://www.ccsdut.org/policies>

Government Records Access and Management Act, Utah Code § 63G-2-101 *et seq.* (1991). <https://le.utah.gov/xcode/Title63G/Chapter2/63G-2.html>

Utah State Board of Education. (2023). *Utah educator professional standards*, Utah Administrative Code R277-515. <https://rules.utah.gov/publicat/code/r277/r277-515.htm>

Utah State Government. (2021). *Utah Code § 63A-16-209: Agency websites—Privacy policy—Security policy*. <https://le.utah.gov/xcode/Title63A/Chapter16/63A-16-S209.html>

Updated: September 1, 2026