Cottonwood School District No. 242

PERSONNEL **5330**

Employee Email and On-Line Services Usage

Internet access and interconnected computer systems may be available to the District's faculty. Electronic networks, including the internet, are a part of the District's instructional program in order to promote educational excellence by facilitating resource sharing, innovation, and communication.

Staff may, consistent with the computer use policies of the District and the District's educational goals, use approved internet sites throughout the curriculum.

The District email and internet systems are provided for educational purposes only. The District's electronic network is part of the curriculum and is not a public forum for general use.

Uses

Use for other informal or personal purposes is permissible within reasonable limits provided it does not interfere with work duties and complies with District policy. All email and internet records are considered District records and should be transmitted only to individuals who have a need to receive them and only relating to educational purposes. Staff has no expectation of privacy in any materials that are stored, transmitted, or received via the District's electronic network or District computers. The District reserves the right to access, monitor, inspect, copy, review, and store, at any time and without prior notice, any and all usage of the computer network and Internet access and any and all information transmitted or received in connection with such usage, including email and instant messages.

Unacceptable Uses of Network

The following are considered examples of unacceptable uses and constitute a violation of this policy. Additional unacceptable uses can occur other than those specifically listed or enumerated herein:

1. Uses that violate the law or encourage others to violate the law including local, State, or federal law; accessing information pertaining to the manufacture of weapons; intruding into the networks or computers of others; and downloading or transmitting confidential, trade secret information, or copyrighted materials;

2. Uses that cause harm to others or damage their property, person, or reputation, including but not limited to engaging in defamation; employing another's password or some other user identifier that misleads message recipients into believing that someone other than you is communicating; reading or sharing another person's communications or personal information; or otherwise using their access to the network or the internet;

3. Uploading a worm, virus, other harmful form of programming or vandalism; participating in "hacking" activities or any form of unauthorized access to other computers, networks, or other information. Staff will immediately notify the school's system administrator if they have identified a possible security problem.

4. Downloading the TikTok app or visiting the TikTok website;

5. Uses amounting to harassment, sexual harassment, bullying, or cyber-bullying (defined as using a computer, computer system, or computer network to convey a message in any format that is intended to harm another individual);

6. Uses that jeopardize the security of access and of the computer network or other networks on the Internet; uses that waste District resources;

7. Uses that are commercial transactions, including commercial or private advertising;

8. The promotion of election or political campaigns, issues dealing with private or charitable organizations or foundations, ballot issues, or proselytizing in a way that presents such opinions as the view of the District;

9. Sending, receiving, viewing, or downloading obscene materials, materials harmful to minors, materials that depict the sexual exploitation of minors, or other inappropriate materials;

10. Sharing one's password with others or allowing them to use one's account;

11. Downloading, installing, or copying software or other files without authorization of the Superintendent or the Superintendent's designee;

12. Posting or sending messages anonymously or using a name other than one's own;

13. Attempting to access the Internet using means other than the District network while on campus or using District property;

14. Sending unsolicited messages such as advertisements, chain letters, junk mail, and jokes;

15. Sending emails that are libelous, defamatory, offensive, or obscene;

16. Notifying patrons or the public of the occurrence of a school election by providing anything other than factual information associated with the election – such as location, purpose, etc. Such factual information shall not promote one position over another;

17. Forwarding or redistributing the private message of an email sender to third parties or giving the sender's email address to third parties without the permission of the sender; and/or

18. Downloading or disseminating copyrighted or otherwise protected works without

permission or license to do so.

Records

District records, including email and internet records may be subject to public records requests, disclosure to law enforcement or government officials, or to other third parties through subpoena or other processes. The Superintendent or their designee may review any and all email of any employee, at any time, with or without cause. Consequently, employees should always ensure that all information contained in email and internet messages is accurate, appropriate, and lawful. When sending student records or other confidential information by email, staff shall be aware of the security risks involved and shall take all steps directed by the building principal to reduce such risks.

The building principal shall provide direction to staff on how to send student records or other confidential information by email in a secure manner.

Email can be used to communicate with parents however, it is important that confidential information about a student never be transmitted via email. A letter, telephone call, or a parent conference may be more appropriate. Please be aware that student-teacher and parent-teacher communication via email is not secure and that any email can become a public record or possibly be obtained by unauthorized users. When communicating with students and parents by email, employees should use their District e-mail rather than a personal email account. Email and internet messages by employees may not necessarily reflect the views of the District. Abuse of the email or internet systems, through excessive and/or inappropriate personal use, or use in violation of the law or District policies, will result in disciplinary action, up to and including termination of employment. E-mail messages and Internet records are to be treated like shared paper files, with the expectation that anything in them is available for review by the Superintendent.

Privacy

While the District does not intend to regularly review employees' email and internet records, employees have no right or expectation of privacy in their use of email or the internet via devices or internet access provided by the District., and the District may review any and all email of any employee, at any time, with or without cause. Employees shall not use the District's equipment, email, network, software, etc. to engage in otherwise confidential communications as there is no right or expectation of privacy in any communication using District property and any such communications are subject to review by District personnel. Depending upon content, email and Internet communications may potentially be disclosed to any member of the public through a public records request. The District owns the computer, networks, and software making up the e-mail and Internet system and permit employees to use them in the performance of their duties for the District.

Internet Access Conduct Agreements

Each staff member will be required to sign the Procedure 5330F Employee Electronic Mail and On-line Services Use Policy Acknowledgment upon the adoption of this policy or upon hiring.

Warranties/Indemnification

The District makes no warranties of any kind, express or implied, in connection with its provision of access to and use of its computer networks and the internet provided under this policy. The District is not responsible for any information that may be lost, damaged, or unavailable when using the network, or for any information that is retrieved or transmitted via the internet. The District will not be responsible for any unauthorized charges or fees resulting from access to the internet, and any user is fully responsible to the District and shall indemnify and hold the District, its Trustees, administrators, teachers, and staff harmless from any and all loss, costs, claims, or damages resulting from such user's access to its computer network and the internet, including but not limited to any fees or charges incurred through purchases of goods or services by the user.

Violations

If any staff member violates this policy, they may be subject to disciplinary action. The system administrator and/or the Internet Safety Coordinator and/or the building principal will make all decisions regarding whether or not a user has violated this policy and any related rules or regulations. Actions which violate local, State, or federal law may be referred to the local law enforcement agency.

Cross Reference:	5290	Political Activity-Staff Participation
	5325	Employee Use of Social Media Sites, Including Personal Sites
Legal Reference:	IC § 18-6726	TikTok Use by State Employees on a State-Issued Device Prohibited
	Idaho Executive Order 2022-06	
	Board of County Commissioners v. Idaho Health Fac. Auth., 531 P.2d 588 (1975)	
Other Reference:	Idaho Attorney General Opinion No. 95-07 ("What are the limitations on Loaning and/or sharing State of Idaho employees or facilities to or with Private charitable foundations?") (available at: https://www.ag.idaho.gov/content/uploads/2017/12/1995.pdf)	

Policy History:
Adopted on: February 22, 2017
Revised on: August 21, 2023