Policy File: GBCBB
West Central School District 49-7

EXPECTED METHODS OF COMMUNICATION BY EMPLOYEES

With the increasing risk of cybersecurity threats, it is imperative that the district provide trusted methods of communication with all our stakeholders. In order to be a trusted method of communication, our stakeholders must be able to easily identify that the source of the communication is legitimate and that its author is speaking on behalf of the district. All district employees are to follow the policy laid out here.

The Superintendent in conjunction with the administrative team will ensure that staff members are periodically informed of the importance of maintaining proper decorum when using any form of communication. As well as the available channels of communication in which they should be interacting with stakeholders.

District managed sites and services:

Stakeholders use a number of methods to determine the legitimacy of communication in order to protect their loved ones and their livelihood. It is important that our staff uses expected and trusted sources. Examples include:

1. A k12.sd.us email account that is protected by multi factor authentication, anti-virus and anti-malware software. Instead of a private 3rd party hosted email account that isn't easily identifiable as originating from the district.
2. A file sharing service such as Google Drive or Microsoft One Drive, which is tied to a k12.sd.us email account. Instead of a private 3rd party hosted account.
3. A video conferencing solution, such as Zoom or Microsoft Teams, which is tied to a k12.sd.us email account.
4. A school provided telephony solution that identifies the call as coming from the West Central School District instead of a privately owned device.
5. A district branded website, mobile app or 3rd party service instead of an equivalent personal web service.

A District managed site or service will be clearly labeled as such. And these managed sites and services will be reviewed for possible policy and copyright violations. Disciplinary action may be imposed for copyright violations. All material posted to a District site or service is subject to review and removal by the administration or designee for violation of copyright or policies. No copyrighted material is to be posted in a way that allows for unlimited viewing of said material via the Internet without proper permission from the copyright holder – this includes student created work. If the student creator is a minor, permission must be received from the student's parent or guardian prior to posting.

Violations of District policy even if contained on a non-district managed site or services are subject to discipline. There will be no links to non-work related content included on a District webpage. Work related content that is not publicly available will be kept off

non-district managed sites and services. Legal liability resides with the individual for a personal site or service. Inappropriate online activity coupled with identification of yourself as a District employee on a third party web site or in social media may result in employee discipline.

For legal protection of our staff, the following proscribed conduct includes:

- Improper fraternization with students via any communication medium.
- Posting items or sending messages containing inappropriate sexual content.
- Posting items or sending messages exhibiting or advocating illegal use of drugs or illegal use of alcohol.
- Posting items or sending messages that violate South Dakota's code of professional ethics.

https://doe.sd.gov/professionalpractices/

All staff are to ensure that classrooms are treated as private areas and that any photography by parents or guardians be limited to their own child or children.

Athletics and Activities related communication:

All contact and messages not initiated through, HUDL, school email or Campus Messenger by the activity supervisors to activity participants shall be sent to the activities director, principal and all activity participants. Messages concerning medical or academic privacy will be copied only to the activities director and the school principal.

The administration will randomly monitor improper use of technology, and may impose sanctions per incident that may include dismissal from employment. Employees have no expectation of privacy with respect to utilization of District property including but not limited to use of district provided wifi connections, nor engagement in social networking sites.

Legal References: SD Administrative Rule 24-08-03

Policy
Adopted: 06/09/2014
Revised: 07/09/2018, 04/11/2022