E-mail Security EHAAC

This policy is to protect the confidentiality and integrity of student, teacher and personally identifiable information (PII) data which may be sent or received via email.
It applies to all Crook County School District #1 work force members including, but not limited to full-time employees, part-time employees, trainees, volunteers, contractors, temporary workers, and anyone else granted access to sensitive information by CCSD#1. All work force members are responsible for the security of protected information.

CCSD#1 recognizes that using email without the use of an encryption mechanism is an insecure means of sending and receiving messages and will utilize the following guidelines regarding sending sensitive information via email:

- Sensitive information should not be sent by email
- Approved alternative methods of delivering sensitive information or PII include SFTP, Wyoming Transcript Center, secured Fusion reports, or shared secured folders
- "Sensitive" is defined as any information that is not readily available to the public under federal or state public records accessibility laws. If a work force member is unsure whether information is sensitive and subject to this policy, he/she must receive approval from a supervisor before sending it in an unencrypted manner
- In the event a CCSD#1 work force member needs to utilize email to send secure information, proper encryption software provided and authorized by the CCSD#1 technology staff must be utilized.

CCSD#1 provided e-mail systems are intended for official and authorized purposes only. E-mail messages are considered to be district property. System administrators and others with special system-level access privileges are prohibited from reading electronic messages of others unless authorized by appropriate CCSD#1 leadership.

All individuals identified in the scope of this policy are responsible to:

- Abide by the terms and guidelines set forth by this policy
- Secure email access to prevent any unauthorized use

Failure to comply with this or any other security policy will result in disciplinary actions as per policy. Legal actions also may be taken for violations of applicable regulations and standards such as state and federal rules to include the Family Educational Rights and Privacy Act (FERPA).

References:

- The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99)
- International Standards Organization (ISO 27002).

Adopted: February 21, 2017