7200 Technology Security

The purpose of this policy is to secure communication devices and data on the Campbell County School District (CCSD) network and to ensure critical information is backed up, protected, and data flow is not interrupted by unauthorized access.

NETWORK SECURITY, DATA BACKUP AND STORAGE, ACCESS CONTROL, ENCRYPTION, AND PASSWORD MANAGEMENT

- Information traveling over District computer networks, not specifically identified as the property of other parties, will be treated as a District asset. It is the policy of the District to prohibit unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft of this information.
- Information belonging to third parties and entrusted to the District in confidence will be protected.
- Data sensitive systems are required to have an exact, retrievable copy. The backed up data must be stored in a secure offsite location and ensure the appropriate access controls are implemented to only allow authorized access to all such data.
- Computer and communications system privileges of all users, systems, and independently operating programs (such as "agents") must be restricted based on a need-to-know basis.
- Confidential information will be maintained to allow access only to those persons or software programs granted access rights as specified by regulation or business process. This will apply to all systems, network, and applications; as well as all facilities which process, store, or transmit confidential information.
- “Data in motion” will be protected by implementing a combination of solutions including Virtual Private Networks (VPNs), Secure Sockets Layer (SSL) and other technologies. Systems will be identified that require confidential information to be encrypted for the purpose of transmission.
- All staff must employ password-based access controls when accessing systems storing or transmitting confidential information.

COMPLIANCE

Failure to comply with this or any other security policy may result in disciplinary actions. 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).

ADOPTION DATE: May 11, 2021, and rescinded prior Policy 3710, Network Security; and rescinded Policy and Administrative Regulation 4510, Technology: Security, Sharing of Resources, Technology Acceptable Use
LEGAL REFERENCE(S): Children's Online Privacy Protection Act (COPPA), Children’s Internet Protection Act, 47 U.S.C. §254 (CIPA); The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) and International Standards Organization (ISO 27002).
CROSS REFERENCE(S): 4374, 4675, 5147, 5276, 5330, 7100, and all sections under 7100-R

ADMINISTRATIVE REGULATION: 7200-R, Sections 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, and 13
ADMINISTRATIVE FORMS: 7200 Form, CCSD System Access Request