7200-R Section 3, Access Control

Campbell County School District will control access to its information assets and systems. Only individuals formally authorized to view or change confidential information will be granted access to that information. Access privileges will be based on the individual's job description.

Access to confidential information will be granted only if an individual has a legitimate business need for the information. Reasonable efforts will be made to limit the amount of information to the minimum necessary needed to accomplish the intended purpose of the use, disclosure, or request.

Each individual accessing confidential information via a District computer will be granted some form of unique user identification, such as a login ID. At no time will any employee allow anyone else to use their unique ID. Likewise, at no time will any employee use anyone else's ID.

Campbell County School District will:

- Develop a standard convention for assigning unique user identifiers;
- Maintain a secure record of unique assigned user identifiers; and
- Track individual activities and record events as required by Administrative Regulation 7200-R, Section 7, Audit Controls.

The District will establish an emergency access procedure for gaining access to confidential information during an emergency. Extraordinary care in safeguarding and documenting the use of the information will be exercised during this procedure.

Wherever reasonable and appropriate, the District will establish role-based categories identifying types of information necessary for employees to do their jobs. Access to confidential information will be granted based on the roles or functions the individual performs within the organization.

The District will maintain procedures for automatic logoff of systems containing confidential information after a period of inactivity. The length of time a user is allowed to stay logged on while idle will depend on the sensitivity of the information accessed.

The District will evaluate and implement encryption and decryption solutions which are deemed financially reasonable and technically sound and useable as an additional form of access control.

RESPONSIBILITIES

- All individuals are responsible for:
  - Ensuring no other individual uses their unique ID,
  - Never using another individual's unique ID, and
  - Abiding by access control guidelines.
- District server administrators are responsible for:

- Ensuring employees have access to only the confidential information they need to do their jobs,
- Creating, maintaining, and controlling access based on the roles and functions workforce members perform in the organization,
- Ensuring each workforce member has a unique user ID for access to systems containing confidential information,
- Maintaining emergency access procedures,
- Maintaining automatic logoff procedures, and
- Evaluating and implementing (when reasonably appropriate) encryption and decryption solutions as a form of access control.

ADOPTION DATE: May 11, 2021
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.
ADMINISTATIVE REGULATION: 7200-R, Sections 1, 2, 4, 5, 6, 7, 8, 9, 10, 11, 12, and 13
ADMINISTRATIVE FORMS: 7200 Form, CCSD System Access Request