7200-R Section 7, Audit Controls

Campbell County School District will identify critical systems requiring event auditing capabilities. The District will define the events to be audited on all such systems. At a minimum, event auditing capabilities will be enabled on all systems processing, transmitting, and/or storing confidential information. Events to be audited may include, but are not limited to; logins, logouts, accessing files, deletions, and modifications.

The District will ensure the protection of all audit reports and log files.

The District will review software and application tools used to review audit files.

When requested, and for the purpose of performing an audit, any access needed will be provided to authorized members of the District. This may include:

- Access to user level and/or system level of computing or communications devices,
- Access to information (electronic, hardcopy, etc.) produced, transmitted, or stored on District equipment or premises,
- Access to work areas (labs, offices, cubicles, storage areas, etc.), and
- Access to interactively monitor and log traffic on District networks.

The designated security officer will be responsible for ensuring the implementation of audit controls.

Audits may be conducted to:

- Ensure confidentiality, integrity, and availability of sensitive information,
- Investigate possible security incidents and ensure conformance to District security policies, and
- Monitor user or system activity where appropriate.

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, 3, 4, 5, 6, 8, 9, 10, 11, 12, and 13