Employee Responsible Use Guidelines for Technology

Clear Creek Independent School District provides various technologies to enhance teaching, support administrative functions, facilitate resource sharing, innovation, and communication. These technologies include District-provided equipment, personal devices (e.g., phones, tablets, laptops), and District-approved applications. By embracing these guidelines, employees will become responsible digital citizens.

Employees are required to **review these guidelines annually**, acknowledge their understanding, and agree to comply. All District technology use is subject to **monitoring**, and there's **no expectation of privacy**.

Core Principles for Technology Use:

- Technology will be used to enhance teaching and learning, and to support District operations, in a meaningful, safe, and responsible way.
- Employees represent the school district in all online activities. Online actions should not reflect negatively on students, colleagues, or the District.
- Employees will use technology resources productively and appropriately for school-related purposes, without disrupting others.
- Employees will use digital communication understanding they are creating a digital reputation.
- District account information is personal and private; employees should **not share it**. Only use your assigned account.
- Employees are responsible for using technology in compliance with academic integrity expectations and professional standards.
- District administrators will determine what conduct constitutes inappropriate use, even if not explicitly specified.

Prohibited Technology-Specific Actions:

- Modifying computer settings or internal/external configurations without permission.
- Tampering with or theft of District technology components.
- Attempting to access or circumvent passwords or other security information of the District, students, or employees.

- Uploading or creating computer viruses.
- Attempting to alter, destroy, or disable District technology resources, data, or other networks.
- Causing network congestion through mass consumption of system resources.
- Using District systems for any income-generating activity, advertising, or promoting non-District affiliated events.
- Transmitting confidential information without proper authorization. **Do not reveal personal information about yourself** (e.g., home address, phone number, email address, birthdate) or others.
- Engaging in **impersonation** (logging on as someone other than yourself).
- Deleting, examining, copying, or modifying files and/or data belonging to other users without their permission.
- Using obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language in digital communications.
- Using District resources for political activities or lobbying.
- Creating, distributing, or forwarding chain letters, spam, or messages not related to educational purposes.
- Using or possessing copyrighted material without appropriate authorization (e.g., sharing unauthorized content, displaying copyrighted videos without permission).

Use of Digital Tools:

- All online actions leave a **permanent record** and remain online, even if deleted.
- Personal use of social media may influence current and future employment opportunities.
- Employees using digital learning tools in their classrooms must **monitor student actions** for compliance with the Student Code of Conduct.
- Employees must ensure digital tools used in the classroom are in accordance with age requirements per the tool’s terms and conditions or privacy policy.
- If using personal social network pages, employees are responsible for their content, including content added by others, and for maintaining appropriate privacy settings.
- Employees are prohibited from knowingly communicating with students through a **personal social network page or site**; a separate "professional page" must be created with prior principal approval.
- All electronic communication with students must be **limited to matters within the scope of professional responsibilities**.

- Upon request from administration, an employee must provide contact information regarding electronic media used to communicate with students.
- Upon written request from a parent or student, the employee **shall discontinue** one-to-one electronic communication with that student.
- An employee shall notify their supervisor in writing within one business day if a student engages in an **improper electronic communication** with the employee.

If the CCISD employee chooses to use generative artificial intelligence (AI) tools:

- Entering passwords or other confidential, proprietary, or sensitive information into any AI system is prohibited. Under no circumstances will student or employee personally identifiable information be used with AI.
- Any AI tools specifically prohibited by the District or law shall not be used.

Use of Personally-Owned Technology Devices at School:

- Internet access on personal devices will be **filtered by the District**. Connection to the filtered, wireless network is required for internet access on campus.
- These devices are the **sole responsibility of the employee user**. The District assumes no responsibility for lost, loaned, damaged, or stolen personal devices.
- Employees are prohibited from trading or selling these items on District property.
- Employees are responsible for their own device's set-up, maintenance, charging, and security. Staff will not diagnose, repair, or store employee personal devices.
- Personal devices are for professional purposes or limited personal use as defined by these guidelines.
- Campus administrators and staff can prohibit device use at certain times, during designated activities, or in designated locations.

Consequences of Violation:

Should an employee commit a violation of these technology guidelines, consequences could include **revocation of technology privileges**, disciplinary action in accordance with District policies, and/or referral to law enforcement. The System Administrator and/or principal may deny, revoke, or suspend access pending investigation.

Disclaimer:

The District’s system is provided "as is, as available." The District does not guarantee uninterrupted or error-free service. While filtering software is in place, controlling all content on the internet is impossible. Opinions, advice, or services expressed by third parties are not those of the District. The District will cooperate fully with law enforcement in any investigation concerning misuse of its system.