CLEAR CREEK
INDEPENDENT SCHOOL DISTRICT

Employee Responsible Use Guidelines for Technology

Introduction

Clear Creek Independent School District makes a variety of communications and information technologies available to students and District employees through computer/network/Internet access. These technologies, when properly used, promote educational excellence in the District by facilitating resource sharing, innovation, and communication within the District. Illegal, unethical or inappropriate use of these technologies can have dramatic consequences, harming the District, its students and its employees. These Responsible Use Guidelines are intended to minimize the likelihood of such harm by educating District students and employees and setting standards which will serve to protect the District. The District firmly believes that digital resources, information and interaction available on the computer/network/Internet far outweigh any disadvantages.

Mandatory Review

To educate District employees and students on proper computer/network/Internet use and conduct, users are required to review these guidelines at the beginning of each school year. All District employees shall be required to acknowledge receipt and understanding of all administrative regulations governing use of the system and shall agree in writing to allow monitoring of their use and to comply with such regulations and guidelines.

Definition of District Technology System

The District’s computer systems and networks (system) are any configuration of hardware and software. The system includes but is not limited to the following:

- Telephones, cellular telephones, and voicemail technologies;
- Email accounts;
- Servers;
- Computer hardware and peripherals;
- Software including operating system software and application software;
- Digitized information including stored text, data files, email, digital images, and video and audio files;
- Internally or externally accessed databases, applications, or tools (Internet- or District- server based);
- District-provided Internet access; and
- New technologies as they become available.

Acceptable Use

Computer/Network/Internet access will be used to improve teaching and learning consistent with the District’s strategic plan and supporting educational goals. The District requires legal, ethical and appropriate computer/network/Internet use.

Access to Computer/Network/Internet

Computer/Network/Internet access is provided to all District teachers and staff. Access to the District’s electronic communications system, including the Internet, shall be made available to students and employees primarily for instructional and administrative purposes and in accordance with administrative regulations. Each District computer and public Wi-Fi has filtering software that blocks access to visual depictions that are obscene, pornographic, inappropriate for students, or harmful to minors, as defined by the federal Children's Internet Protection Act (CIPA). Filtered Internet access is provided to students as defined by CIPA. For students under the age of 13, CIPA requires additional parental permission for some Web tools used for educational purposes. Parents wishing to deny access to these sites must do so in writing.

Limited personal use is permitted if the use imposes no tangible cost to the District, does not unduly burden the District's computer or network resources, and has no adverse effect on an employee's job performance or on a student's academic performance.

All individual users of the District's system must complete and sign an agreement to abide by District policies and administrative regulations regarding such use. All such agreements will be maintained on file in either the principal's, departmental supervisor's office, or district human resources department. System users are required to maintain password confidentiality by not sharing their password with others. System users may not use another person's system account. Any system user identified as a security risk or having violated the District's Responsible Use Guidelines may be denied access to the District's system. Other consequences may also be assigned.

Approved Mobile Devices

Employees may access district email from personally owned devices. However, be aware that all policies related to access to CCISD systems still apply. The CCISD Help Desk will not support personally owned mobile devices, however information can be found on the employee portal to set up a personally owned device.

Objectionable Content/Third-Party Supplied Information

System users and parents of students with access to the District's system should be aware that use of the system may provide access to other electronic communication systems in the global electronic network that may contain inaccurate and/or objectionable material. An employee who knowingly brings prohibited materials into the school's electronic environment will be subject to disciplinary action in accordance with District policies. [See Board policy DH]

Subject to Monitoring

All District computer/network/Internet usage shall not be considered confidential and is subject to monitoring by designated staff at any time to ensure appropriate use. System users should not use the computer system to send, receive or store any information, including e-mail messages, that they consider personal or confidential and wish to keep private. All electronic files, including email messages, transmitted through or stored in the computer system will be treated no differently than any other electronic file. The District reserves the right to access, review, copy, modify, delete or disclose such files for any purpose. Users should treat the computer system like a shared or common file system with the expectation that electronic files, sent, received or stored anywhere in the computer system, will be available for review by any authorized representative of the District for any purpose.

User Responsibilities

Staff and student users are responsible for his/her own actions while accessing technology resources. Users are responsible for ensuring system integrity by not acting on any emails or phone calls requesting information about user accounts or any other personally identifiable information. Users should also refrain from clicking on any unexpected hyperlinks or email attachments and sharing internet protocol (IP) addresses.

CCISD Technology will not contact staff or students requesting that a form be filled out to maintain access to any services, nor will CCISD Technology contact users via phone or email to allow unsolicited remote access to any CCISD owned device. Users should contact the CCISD Technology Helpdesk at helpdesk@ccisd.net or 281.284.4357 if these situations occur.

Employee Responsibilities

District employees are bound by all portions of the District's Responsible Use Guidelines. An employee who knowingly violates any portion of the Responsible Use Guidelines will be subject to disciplinary action in accordance with District policies. [See Board policy DH]

Campus- and Departmental-Level Responsibilities

The principal/departmental administrator or designee will:

1. Disseminate and enforce the District's Responsible Use Guidelines for the District's system at the campus or departmental level.
2. Ensure that all individual users of the District's system complete and sign an agreement to abide by District policies and administrative regulations regarding such use.
3. Ensure that employees supervising students who use the District's systems provide information emphasizing digital citizenship focusing on the appropriate, safe, and ethical use of the District's systems to students.
4. Monitor all users of the District's systems to ensure appropriate and ethical use.
5. Use the District's student management system to identify students whose internet use has been restricted and inform staff members who are responsible for these students.

Teacher Responsibilities

The teacher will:

1. Provide age-appropriate lessons in Internet safety and cyber security for students throughout the year, emphasizing digital citizenship.
2. Review responsibilities as users of the District computer/network/Internet prior to gaining access to such system.
3. Comply with federal and state law as well as local policy regarding confidentiality of student information.
4. Review electronic mail guidelines.
5. Verify the list of students who have access to the Internet through the reporting feature in the student management system.
6. Provide developmentally-appropriate guidance to students as they use electronic resources related to instructional goals.
7. Use computer/network/Internet in support of instructional goals.
8. Provide alternate activities, if necessary, for students whose access to the internet has been restricted.
9. Address student violations of the District's Responsible Use Guidelines as defined in the Student Code of Conduct.
10. Seek prior approval for websites that will be used for educational purpose for students under the age of 13 in which account will be created for student logins and abide by the following guidelines such as CIPA and COPA:

- Review the website's privacy policy to identify how and what student information is collected. If a website collects personal information beyond students' names (First Name and Last Initial) and district provided email address, the site must be submitted for approval prior to using with students.
- Prior to creating any student accounts, receive written permission from parents that includes written communication about the website URL, student outcomes, how students will access the program, and any other relevant information that will support the use of the website for student learning.

Clear Creek ISD Employee Code of Conduct

District employees are expected to maintain appropriate conduct when accessing the communications and information technologies available through computer/network/Internet access. All employees must comply with the District's Responsible Use Guidelines at all times when accessing any part of the technology system.

Employees will guard and protect access to secure systems by:

1. **Protecting passwords and other similar authorization information:** Passwords are the primary way in which users are authenticated and allowed to use the District's computing resources. Employees will not disclose personal password(s) to any individual, including a faculty or staff member. Similarly, employees will not disclose other identifying information used to access specific system information, recognizing that if they do so, they will be held accountable for their actions as well as those of other parties to whom they have given access.
2. **Guarding unauthorized use of resources:** Employees will not allow others to make use of their accounts or network access privileges to gain access to resources to which they would otherwise be denied.
3. **Not circumventing or compromising security:** Employees must not utilize any hardware or software in an attempt to compromise the security of any other system, whether internal or external to the District's systems and network.

Computer/Network/Internet usage is subject to monitoring by designated staff at any time to ensure appropriate use. Electronic files sent, received or stored anywhere in the computer system are available for review by any authorized representative of the District for any purpose. Employees will affirm, in writing that at all times their actions while using the District's system will not violate the law or the rules of network etiquette, will conform to the guidelines set forth in the Responsible Use Guidelines, and will not violate or hamper the integrity or security of the District's technology system.

If a violation of the Responsible Use Guidelines occurs, employees will be subject to one or more of the following actions:

1. Revocation of access;
2. Disciplinary action;
3. Loss of employment with the District;
4. Appropriate legal action.

Use of Social Networking/Digital Tools

Students and employees may participate in District-approved social media learning environments related to curricular projects or school activities and use digital tools, such as, but not limited to, mobile devices, blogs, discussion forums, RSS feeds, podcasts, wikis, and on-line meeting sessions.

The use of blogs, wikis, podcasts, and other digital tools are considered an extension of the classroom. Verbal or written language that is considered inappropriate in the classroom is also inappropriate in all uses of blogs, wikis, podcasts, and other district-approved digital tools. Employees who use digital learning tools in their classrooms must monitor student actions to ensure compliance with the Student Code of Conduct.

Inappropriate Use

Inappropriate use includes, but is not limited to, those uses that violate the law, that are specifically named as violations in this document, that violate the rules of network etiquette, or that hamper the integrity or security of this computer/network/Internet system or any components that are connected to it. The following actions are considered inappropriate uses and are prohibited:

Violations of Law

Transmission of any material in violation of any federal or state law is prohibited. This includes, but is not limited to:

- unauthorized disclosure of confidential student information protected by the Family Educational Rights Privacy Act
- threatening, harassing, defamatory or obscene material;
- copyrighted material;
- plagiarized material; or
- material protected by trade secret.

Tampering with or theft of components from District systems may be regarded as criminal activity under applicable state and federal laws. Any attempt to break the law through the use of a District computer/network/Internet account may result in prosecution against the offender by the proper authorities. If such an event should occur, the District will fully comply with the authorities to provide any information necessary for the litigation process.

Intellectual Property

Teachers, staff and students must always respect copyrights and trademarks of third parties and their ownership claims in images, text, video and audio material, software, information and inventions. The copy, use, or transfer of others' materials without appropriate authorization is not allowed.

Transmitting Confidential Information

Teachers, staff and students shall not redistribute or forward confidential information (i.e. educational records, directory information, personnel records, etc.) without proper authorization. Confidential information should never be transmitted, redistributed or forwarded to outside individuals who are not expressly authorized to receive the information. Revealing personal information such as, but not limited to, home addresses, phone numbers, e-mail addresses, birthdates of users or others is prohibited.

Modification of Computer

Modifying or changing computer settings and/or internal or external configurations without appropriate permission is prohibited.

Commercial Use
Use of the system for any type of income-generating activity is prohibited. Advertising the sale of products, whether commercial or personal is prohibited.

Marketing by Non-CCISD Organizations
Use of the system for promoting activities or events for individuals or organizations not directly affiliated with or sanctioned by the District is prohibited.

Vandalism/Mischief
Any malicious attempt to harm or destroy District equipment, materials or data; or the malicious attempt to harm or destroy data of another user of the District's system, or any of the agencies or other networks to which the District has access is prohibited. Deliberate attempts to degrade or disrupt system performance are violations of District policy and administrative regulations and may constitute criminal activity under applicable state and federal laws. Such prohibited activity includes, but is not limited to, the uploading or creating of computer viruses.

Vandalism as defined above is prohibited and will result in the cancellation of system use privileges. System users committing vandalism will be required to provide restitution for costs associated with system restoration and may be subject to other appropriate consequences. [See DH, FN series, and FO series in Board Policy and the Board-approved Student Code of Conduct.]

Impersonation/Plagiarism
Fraudulently altering or copying documents or files authored by another individual or assuming the identity of another individual is prohibited.

Illegally Accessing or Hacking Violations
Intentional or unauthorized access or attempted access of any portion of the District's computer systems, networks, or private databases to view, obtain, manipulate, or transmit information, programs, or codes is prohibited.

File/Data Violations
Deleting, examining, copying, or modifying files and/or data belonging to other users, without their permission is prohibited.

Copyright Violations
Downloading or using copyrighted information without following approved District procedures is prohibited.

System Interference/Alteration
Deliberate attempts to exceed, evade or change resource quotas are prohibited. The deliberate causing of network congestion through mass consumption of system resources is prohibited.

Electronic Mail and Communication Tools
Electronic mail (e-mail) and other digital tools such as, but not limited to, blogs and wikis, are tools used to communicate within the District. The use of these communication tools should be limited to instructional, school-related activities, or administrative needs.

Users should keep the following points in mind:

Perceived Representation
Using school-related e-mail addresses, blogs, wikis, and other communication tools might cause some recipients or other readers of the e-mail to assume that the user’s comments represent the District or school, whether or not that was the user’s intention.

Privacy
E-mail, blogs, wikis, and other communication within these tools should not be considered a private, personal form of communication. Private information, such as home addresses, phone numbers, last names, pictures, e-mail addresses, or student ID numbers should not be divulged. To avoid disclosing e-mail addresses that are protected, all e-mail communications to multiple recipients should be sent using the blind carbon copy (bcc) feature.

Inappropriate Language
Using obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language in e-mails blogs, wikis, or other communication tools is prohibited. Sending messages that could cause danger or disruption, personal attacks, including prejudicial or discriminatory attacks are prohibited.

Political Lobbying
Consistent with State ethics laws, District resources and equipment, including, but not limited to, e-mails, blogs, wikis, or other communication tools must not be used to conduct any political activities, including political advertising or lobbying. This includes using District e-mail, blogs, wikis, or other communication tools to create, distribute, forward, or reply to messages, from either internal or external sources, which expressly or implicitly support or oppose a candidate for nomination or election to either a public office or an office of a political party or support or oppose an officeholder, a political party, or a measure (a ballot proposition). These guidelines prohibit direct communications as well as the transmission or forwarding of e-mails, hyperlinks, or other external references within e-mails, blogs, or wikis regarding any political advertising.

Forgery
Forgery or attempted forgery of e-mail messages is prohibited. Attempts to read, delete, copy or modify the e-mail of other system users, deliberate interference with the ability of other system users to send/receive e-mail, or the use of another person’s user ID and/or password is prohibited.

Junk Mail/Chain Letters
Generally, users should refrain from forwarding e-mails which do not relate to the educational purposes of the District. Chain letters or other e-mails intended for forwarding or distributing to others is prohibited. Creating, distributing or forwarding any annoying or unnecessary message to a large number of people (spamming) is also prohibited.

Display of Student Information on District-approved Websites

The following conditions apply to the display of student information on District, campus or teacher Web sites. A content contributor who knowingly violates (or promotes the violation of) any portion of these guidelines will be subject to disciplinary action in accordance with District policies. [See Board policy DH]

- Student-created projects, writings, and/or artwork are permitted on campus/District Web sites, or District-approved blog and wiki sites, if the appropriate parental consent has been obtained.
- Student photographs are permitted only if the appropriate consent has been obtained.
- All student photographs and/or student work must be displayed with either no name, first name only, or first name and last initial only. No other personal student information is allowed including, but not limited to, parents' name, e-mail address, phone number, home address, and/or age or birth date.

Security Reporting/Security Problem

If knowledge of inappropriate material or a security problem on the computer/network/Internet is identified, the user should immediately notify the District's Help Desk. The security problem should not be shared with others.

Impersonation

Attempts to log on to the computer/network/Internet impersonating a system administrator or District employee, student, or individual other than oneself, will result in revocation of the user's access to computer/network/Internet.

Other Security Risks

Any user identified as having had access privileges revoked or denied on another computer system may be denied access to the District computer/network/Internet.

Consequences of Agreement Violation

Any attempt to violate the provisions of this agreement may result in revocation of the user's access to the computer/network/Internet, regardless of the success or failure of the attempt. In addition, school disciplinary action and/or appropriate legal action may be taken.