Ceres Unified School District

STAFF TECHNOLOGY USE POLICY

PURPOSE

In accordance with BP 4040 and AR 4040, the District provides various Technology Resources to authorized employees to assist them in performing their job duties for the District. Each employee has a responsibility to use the District's Technology Resources in a manner that increases productivity, enhances the District's public image, and is respectful of other employees. Technology Resources consist of all electronic devices, software, and means of electronic communication, including, but not limited to, the following, whether provided or supported by the District: personal computers and workstations; laptop computers; mini and mainframe computers; computer hardware such as disk drives and tape drives; peripheral equipment such as printers, modems, fax machines, and copiers; computer software applications and associated files and data, including software that grants access to external services, such as the Internet; electronic mail; telephones; cellular phones; pagers; and voicemail systems. Failure to follow the District's policies regarding its Technology Resources may lead to disciplinary measures, up to and including termination of employment.

I. GENERAL PROVISIONS

A. Use of District Technology Resources

The District provides employees with access to Technology Resources to assist them in performing their duties. The District expects that when employees use Technology Resources during work hours, while on the District's premises, or remotely through the use of the District's computer equipment, they will do so in a responsible manner and for work-related purposes only. The District expects employees to exercise discretion and good judgment when using Technology Resources, or when sending or receiving electronic mail and attachments thereto. Improper use of the District's Technology Resources may lead to discipline, including, but not limited to, discharge from employment. Improper use of the Internet or electronic mail includes, but is not limited to, the following:

1. Use which is illegal, which is contrary to the District's best interests, or which violates or conflicts with the District's policies, including, but not limited to, the District's policies against discrimination or harassment.
2. Use which discloses or leads to the unauthorized disclosure of confidential information.
3. Use of electronic mail, chat rooms or other Internet devices that is defamatory or offensive in any way, including, but not limited to, racially or sexually charged messages, jokes or cartoons.
4. Use of Internet sites, which may damage or interfere with the District's computer network, including use that generates the delivery of "junk" electronic mail.
5. Use that violates copyright laws.
6. Personal use and/or use which is not work-related, as further detailed below.
7. Responding to spam and/or phishing email by giving out your login information including passwords.

B. Confidential Information

The District is very sensitive to the issue of protection of student and employee information and other confidential information of both the District and third parties ("Confidential Information"). Therefore, employees are expected to use good judgment and to adhere to the highest ethical standards when using or transmitting Confidential Information on the District's Technology Resources. Confidential information should not be accessed through the District's Technology Resources in the presence of unauthorized individuals. Similarly, Confidential Information should not be left visible or unattended.

C. Social Networking

Personal correspondence with students on social networking sites, chat rooms, and other Internet services from a private technology resource is discouraged and should be used with discretion. Nevertheless, employees are reminded to ensure any correspondence on social networking sites, chat rooms, and other Internet services from private technology resources is age appropriate and to avoid posting inappropriate or offensive content that does not enhance the integrity of the District and the goals of the educational program in violation of the Code of Ethics Board Policy 4119.21, 4219.21, and 4319.21.

D. Retention of Electronic Records

All district-related electronically stored information generated or received by a district employee that constitutes a district record that is required to be retained by law shall be saved to an electronic file on the district's computer and retained for at least 180 days, or shall be printed by the employee and physically filed in a way that it can be easily retrieved when needed. District-related electronically stored information includes, but not limited to, any email, voicemail, text message, word processing document, spreadsheet, or text document related to district business or generated in the course of an employee's official duty.

E. Software License Restrictions

All software in use on the District's Technology Resources is officially licensed software. No software is to be installed or used that has not been duly paid for and licensed appropriately for the use to which it is being put. No employee may load any software on the District's computers, by any means of transmission, unless authorized in writing in advance by the Director of Information Technology Services**.**

F. Internet Applications

Websites as well as Internet applications, often referred to as "apps", collect different amounts of information. When a user agrees to the terms of service of a website or app, they are entering into an agreement with that company as a representative of the district. To protect staff and students information, staff may neither download any apps nor create staff or students accounts with any application that connects to the Internet without district approval. Reference the *District Approved App. List* to view resources that meet the CUSD data privacy and security requirements.

G. Authorization

Access to the District's Technology Resources is within the sole discretion of the District. Generally, employees are given access to the District's various technologies based on their job functions. Only employees whose job performance will benefit from the use of the District's Technology Resources will be given access to the necessary technology.

H. Personal Use

The District does not provide support of personal devices, often referred to as "Bring Your Own Device" (BYOD). The District's Technology Resources are to be used by employees only for the purpose of conducting business. Employees may, however, use the District's Technology Resources for the following incidental personal uses so long as such use does not interfere with the employee's duties, is not done for pecuniary gain, does not interfere with the performance of job duties or conflict with the District's business, and does not violate any District policy:

1. To send and receive necessary and occasional personal communications;

2. To prepare and store incidental personal data (such as personal calendars, personal address lists, and similar incidental personal data) in a reasonable manner;

3. To use the telephone system for brief and necessary personal calls; and

4. To access the Internet for brief personal searches and inquiries during meal times or other breaks, or outside of work hours, provided that employees adhere to all other usage policies.

The District acknowledges that employees may, at other times, engage in incidental personal use of the Internet, as long as such use does not interfere with the performance of job duties.

I. Limitation of Liability

The District assumes no liability for loss, damage, destruction, alteration, disclosure, or misuse of any personal data or communications transmitted over or stored on the District's Technology Resources. The District accepts no responsibility or liability for the loss or non-delivery of any personal electronic mail or voicemail communications or any personal data stored on any District property. The District strongly discourages employees from storing any personal data on any of the District's Technology Resources.

II. DISTRICT ACCESS TO TECHNOLOGY RESOURCES

A. Property

All messages sent and received, including personal messages, and all data and information stored on the District's electronic mail system, voicemail system or other computer systems/resources are District property regardless of the content. As such, the District reserves the right to access all of its Technology Resources including its computers, voicemail and electronic mail systems, at all time, in its sole discretion.

B. Privacy

Although the District does not wish to examine personal information of its employees, on occasion the District may need to access any and all information on in its Technology Resources, including computer files, electronic mail messages, and voicemail messages. Employees should understand, therefore, that they have no right to privacy with respect to any information or messages created, received or maintained on the District's Technology Resources. The District may, at its discretion, inspect all files or messages on its Technology Resources at any time for any reason. The District may also monitor its Technology Resources at any time to determine compliance with its policies, for purposes of legal proceedings, to investigate misconduct, to locate information, or for any other business purpose.

C. Passwords

Most of the District's Technology Resources can be accessed only by entering a password. Passwords are intended to prevent unauthorized access to information. Passwords do not confer any right of privacy upon any employee of the District. Thus, even though employees may maintain passwords for accessing Technology Resources, employees must not expect that any information maintained on Technology Resources, including electronic mail and voicemail messages, is private. Employees are expected to maintain their passwords as confidential. Employees must not share passwords and must not access coworkers' systems without express authorization.

D. Data Collection

The best way to guarantee the privacy of personal information is not to store or transmit it on the District's Technology Resources. To ensure that employees understand the extent to which information is collected and stored, below are examples of information currently maintained by the District. The District may, however, in its sole discretion and at any time, alter the amount and type of information that it retains.

1. Telephone Use and Voicemail: Records are kept of all calls made from and to a given telephone extension. Although voicemail is password protected, an authorized administrator can reset the password and listen to voicemail messages.

2. Electronic Mail: Electronic mail is backed-up and archived. Although electronic mail is password protected, an authorized administrator can reset the password and read electronic mail.

3. Desktop Facsimile Use: Copies of all facsimile transmissions sent and received are maintained in the facsimile server.

4. Document Use: Each document stored on District computers has a history, which shows which users have accessed the document for any purpose.

5. Internet Use: The District stores records of the Internet sites visited, the number of times visited, and the total time connected to each site is recorded and periodically monitored.

E. Deleted Information

Deleting or erasing information, documents, or messages maintained on the District's Technology Resources is, in most cases, ineffective. All employees should understand that any information kept on the District's Technology Resources may be electronically recalled or recreated regardless of whether it may have been "deleted" or "erased" by an employee. Because the District periodically backs-up all files and messages, and because of the way in which computers re-use file storage space, files and messages may exist that are thought to have been deleted or erased. Therefore, employees who delete or erase information or messages should not assume that such information or messages are confidential.