Cambrian School District

EMPLOYEE TECHNOLOGY RESPONSIBLE USE AGREEMENT

The Employee Technology Responsible Use Agreement is to ensure a clear understanding as to an employee's responsibility with the use of technology resources in Cambrian School District (*Board Policy 4040).* In addition, the intent is to prevent unauthorized access and other unlawful activities by users online, prevent unauthorized disclosure of or access to sensitive information, and to comply with legislation including, but not limited to, the Children's Internet Protection Act (CIPA), Children's Online Privacy Protection Act (COPPA) and Family Educational Rights and Privacy Act (FERPA).

The Cambrian School District provides various Technology Resources to assist employees in performing their job duties for the District. Each employee has a responsibility to use the District's Computer Network and Technology Resources in a manner that increases productivity, enhances the District, and is respectful of other employees.

1. ***Technology Resources:*** Technology Resources consist of all electronic devices, software, and means of electronic communication including, but not limited to, computers; Computer hardware such as disk drives; Other 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; email; telephones; Cellular phones; and voicemail systems.

2. ***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.

3. ***Use****:* The District's Technology Resources are to be used by employees primarily for the purpose of conducting District business. Employees may, however, use the District's Technology Resources for the following personal uses so long as such use does not interfere with the employee's duties, is not illegal, does not conflict with the District's business, and does not violate any District policy:

   A. To send and receive necessary and occasional personal communications.

   B. To use the telephone system for brief and necessary local personal calls.

   C. 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 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.

4. ***Improper Use:***

   A. *Prohibition Against Harassing, Discriminatory and Defamatory Use:* The District is aware that employees use electronic mail for correspondence that is less formal than written memoranda. Employees must take care, however, not to let informality degenerate into improper use. As set forth more fully in the District's Policies on Nondiscrimination (4030) and Sexual Harassment (4030.2), the District does not tolerate discrimination or harassment based on race, creed, color, religion, gender, sexual orientation, national origin, ancestry, physical handicap, marital status, political advocacy, teacher advocacy or age or any other status protected by state and federal laws. Under no circumstances may employees use the District's Technology Resources to transmit, receive, or store any information that is discriminatory, harassing, or defamatory in any way including, without limitation, sexually explicit, racial or otherwise inappropriate messages, jokes or cartoons.

   B. *Prohibition Against Violating Copyright Laws:* Employees must not use the District's Technology Resources to copy, retrieve, forward or send copyrighted materials unless the employee has the author's permission or is accessing a single copy only for the employee's reference.

   C. *Other Prohibited Use:* Employees may not use any of the District's Technology Resources for any illegal purpose, violation of any District policy, in a manner contrary to the best interests of the District, in any way that discloses confidential or proprietary information of the District or third parties, or for personal or pecuniary gain.

5. ***District Access to Technology Resources****:* All messages sent and received, including personal messages, and all data and information stored on the District's email system, voicemail system, or computer systems 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, email systems, and social media accounts, at any time, in its sole discretion.

   A. *Privacy:* Users should have no expectation of privacy regarding their use of District equipment, network, and/or Internet access or files, including email. On occasion, the District may need to access its Technology Resources including computer files, email messages, voicemail messages, etc. 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 computer network and Technology Resources at any time in order to determine compliance

with its policies, for purposes of legal proceedings, to investigate misconduct, to locate information, or for any other business purpose.

B. *Passwords:* Certain 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 email and voicemail messages, are private. Employees are expected to maintain their passwords as confidential, except that all passwords must be disclosed to the systems administrator. Employees must not share passwords and must not access coworkers' systems without express authorization.

C. *Data Collection:* The best way to guarantee the privacy of personal information is not to store or transmit it on the District's network. 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*: Although voicemail is password protected, an authorized administrator can reset the password and listen to voicemail messages. Personal calling cards must be used when making toll or long distance calls of a personal nature. Staff are expected not to use personal devices for non-educational purposes during their job assignment.

   2) *Email*: The District, in its discretion, may back-up and archive electronic mail. Although electronic mail is password protected, an authorized administrator can reset the password and read electronic mail.

   3) *Document Use*: Each document stored on District computers has a history that shows which users have accessed the document for any purpose.

   4) *Internet Use*: Internet sites visited, the number of times visited, and the total time connected to each site is recorded and periodically monitored.

D. *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 of the way in which computers reuse 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.

6. ***The Internet and Online Services:***

   A. *Use of the Internet:* The District provides authorized employees access to online services such as the Internet. The District expects that employees will use these services in a responsible way and primarily for district related purposes. Under no circumstances are employees permitted to use the District's Technology Resources to intentionally access, download, or contribute to indecent or sexually oriented materials, materials relating to the planning of criminal activities or terrorist acts, materials incorporating the use of profanity, gambling sites, illegal drug oriented sites, political lobbying, materials that would violate the District's Policies on Nondiscrimination or Harassment or other inappropriate materials. The District may, in its discretion, use a filtering or other system to limit access to inappropriate materials and web sites.

   Additionally, employees should exercise professional judgement and caution when signing in to "guest books" on Web sites or posting messages to Internet news groups, discussion or social groups, or chatting on Web sites. These actions may generate junk electronic mail and may expose the District to liability or unwanted attention because of comments that employees may make. The District strongly encourages employees who wish to access the Internet for non-work related activities to get their own personal Internet access accounts.

   B. *Confidentiality:* Some of the information to which employees have access is confidential. Employees should avoid sending confidential information over the Internet. Employees also should verify electronic mail addresses before transmitting any messages.

   C. *Monitoring:* The District, in its discretion, may monitor both the amount of time spent using online services and the sites visited by individual employees. The District reserves the right to limit such access by any means available to it, including revoking access altogether. If you are supervising students using technology, please be vigilant in order to ensure students are meeting the provisions outlined in their Student Technology Use Agreement.

   D. *Digital Citizenship:* Employees are responsible for modeling and actively practicing positive digital citizenship. Employees using classroom technology are expected to teach students about positive digital citizenship utilizing resources provided by the district. What employees do and post online must not disrupt school activities or compromise school safety and security.

7. ***Software Use:*** All software in use on the District's network is officially licensed software. No software is to be installed, copied 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 advance by the Director

of Information Technology. Software may not be loaded onto the District's computers until the software to be loaded has been thoroughly scanned for viruses.

8. ***Confidential Information****:* The District is very sensitive to the issue of protection of confidential information of the District, students, parents, and other 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 in the presence of unauthorized individuals and should not be left visible or unattended.

9. ***Security*****:** The District has installed a variety of programs and devices to ensure the safety and security of the District's Technology Resources. Use on the District's computer network or in conjunction with other Technology Resources of computers owned and operated by employees must be approved in advance by the Cambrian School District. All such computers must be protected by industry standard and District approved anti-virus and spyware products.

10. ***Copyright:*** While there are fair use exemptions (http://www.copyright.gov/fls/fl102.html), all users must respect intellectual property. Follow all copyright guidelines (http://copyright.gov/title17/) when using the work of others.

11. ***Cyberbullying:*** Bullying in any form, including cyberbullying, is unacceptable both in and out of school. Please report all cases of bullying to the site administrator or immediate supervisor.

12. ***Professional Language:*** Use positive professional language in all work-related communications.

Employee Technology Responsible Use Agreement Signature Form

After reading the attached information in the Employee Technology Responsible Use Agreement, sign below and return this Employee Technology Responsible Use Agreement Signature Form to your supervisor or other designated administrator.

I have read, understand, and agree to abide by the provisions of the Employee Technology Responsible Use Agreement for the Computer Network and Technology Resources of Cambrian School District.

First Name (print):_____Last Name (print): _____

Employee Signature: _____

Date:_____School/Location: _____

It is required for all employees using the District's computer network and/or technology resources to have a signed agreement form on file.