PERSONNEL

Employee Use of Technology Resources

I. Use

As provided in Section III of Board Policy 4040, the District's Technology Resources are to be used by employees only for the purpose of conducting District 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 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 personal calls; and

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.

All employees may be required to sign Cambrian School District's Technology Acceptable Use agreement.

II. District Access to Technology Resources.

A. *Privacy.* On occasion, the District may need to access its Technology Resources including, but not limited to, computer files, email, text messages, instant messaging, and other electronic communications, even when provided their own password. Employees should understand, therefore, that they have no right of privacy with respect to any messages or information created or maintained on the District's Technology Resources, including personal information or messages. 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 in order to determine compliance with its policies, for purposes of legal proceedings, to investigate misconduct, to locate information, or for any other business purposes.

B. *Passwords.* Certain 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, 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 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.

    a. *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.

    b. *Electronic Mail* - 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.

    c. *Document Use* - Each document stored on District Technology Resources has a history, which shows which users have accessed the document for any purpose.

    d. *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.

III. The Internet and On-Line Services

A. *Use of the Internet*. Employees must not sign "guest books" on Web sites or post messages to Internet news groups, discussions, chat rooms or other online services such social networking platforms**.** 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 on-line 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.

IV. Software Use

All software in use on the District's Technology Resources shall be 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 Technology. Software may not be loaded onto the District's computers until the software to be loaded has been thoroughly scanned for viruses.

V. Confidential Information

The District is very sensitive to the issue of protection of confidential information of both the District and 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 through the District's Technology Resources in the presence of unauthorized individuals. Similarly, Confidential Information should not be left visible or unattended. Moreover, any Confidential Information transmitted via Technology Resources should be marked with the following confidentiality legend: "This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please notify the system manager. This message contains confidential information and is intended only for the individual named. If you are not the named addressee you should not disseminate, distribute or copy this e-mail. Please notify the sender immediately by e-mail if you have received this e-mail by mistake and delete this e-mail from your system. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited."

VI. Security

Use of the District’s computer network or other Technology Resources in conjunction with technology owned and operated by employees such as computers or smart phones must be approved in advance by the Cambrian School District. All such technology resources must be protected by industry standard and District approved anti-virus and spyware products, when applicable.