

CAMBRIAN SCHOOL DISTRICT
Board Policy

Policy 4040
Adopted: September 3, 2020
Page 1 of 4

PERSONNEL

Employee Use of Technology Resources

The Governing Board recognizes that Technology Resources enhance employee performance by offering effective tools to assist in providing a quality instructional program; facilitating communications with parents/guardians, students, and the community; supporting district and school operations; and improving access to and exchange of information. The Board expects all employees to learn to use the available Technology Resources that will assist them in the performance of their job responsibilities. As needed, employees shall receive professional development in the appropriate use of these resources.

Failure to follow the District's policies regarding its Technology Resources may lead to disciplinary measures, up to and including termination of employment. Moreover, the District reserves the right to advise appropriate legal authorities of any violation of law by an employee.

I. Technology Resources Definition

Technology Resources include, but are not limited to, computers, the district's computer network including servers and wireless computer networking technology (Wi-Fi), the Internet, email, USB drives, wireless access points (routers), tablet computers, smartphones and smart devices, telephones, cellular telephones, personal digital assistants, pagers, MP3 players, wearable technology, any wireless communication device including emergency radios, and/or future technological innovations, whether accessed on or off site or through district-owned or personally owned equipment or devices.

II. 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.

III. Use

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 authorized 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.

Employees shall be notified that records maintained on any personal device or messages sent or received on a personal device that is being used to conduct district business may be subject to disclosure, pursuant to a subpoena or other lawful request.

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.

The Superintendent or designee shall establish an Acceptable Use Agreement which outlines employee obligations and responsibilities related to the use of district technology. Upon employment and whenever significant changes are made to the district's Acceptable Use Agreement, employees shall be required to acknowledge in writing that they have read and agreed to the Acceptable Use Agreement.

I. Improper Use

Employees shall report any security problem or misuse of district technology to the Superintendent or designee.

- A. *Prohibition Against Harassing, Discriminatory and Defamatory Use.* As set forth more fully in the District's Policies on Non-Discrimination (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.
- 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. *Harmful or Inappropriate Matter.* Employees shall not use the District's Technology Resources to access, post, submit, publish, or display harmful or inappropriate matter that is threatening, obscene, disruptive, sexually explicit, or unethical or that promotes any activity prohibited by law, Board policy, or administrative regulations.

Harmful matter includes matter, taken as a whole, which to the average person, applying contemporary statewide standards, appeals to the prurient interest and is matter which depicts or describes, in a patently offensive way, sexual conduct and which lacks serious literary, artistic,

political, or scientific value for minors. (Penal Code 313)

- D. *Other Prohibited Uses.* 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.

Inappropriate use of district technology may result in a cancellation of the employee's user privileges, disciplinary action, and/or legal action in accordance with law, Board policy, and administrative regulation.

II. District Access to Technology Resources

All messages sent and received, including personal messages, and all data and information stored on the District's Technology Resources, including, but not limited to, computer files, email, text messages, instant messaging, and other electronic communications are District property regardless of the content. As such, the District reserves the right to access all of its Technology Resources, at any time, in its sole discretion.

The Superintendent or designee shall annually notify employees in writing that they have no reasonable expectation of privacy in the use of any equipment or other Technology Resources provided by or maintained by the district, including, but not limited to, computer files, email, text messages, instant messaging, and other electronic communications, even when provided their own password. To ensure proper use, the Superintendent or designee may monitor employee usage of the District's Technology Resources at any time without advance notice or consent and for any reason allowed by law.

III. The Internet and On-Line Services

The District provides authorized employees access to on-line services such as the Internet. The District expects that employees will use these services in a responsible way and for business-related purposes only. 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 Non-Discrimination 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. The District reserves the right to limit employee access to the Internet or other Technology Resources 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, **copied** or used that has not been duly paid for and licensed

appropriately for the use to which it is being put.

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.

VI. Security

Any employee found tampering or disabling any of the District's security programs or devices will be subject to discipline up to and including termination.

VII. Audits

The District may perform auditing activities or monitoring to determine compliance with these policies. Audits of software and data stored on the District's Technology Resources may be conducted without warning at any time. Employees will not obstruct District representatives' access to Technology Resources for purposes of performing such audit or otherwise monitoring compliance with District policies.