

[Table of Contents](#)**TECHNOLOGY ACCEPTABLE USE****CQ-R***Aligned with the Children's Internet Protection Act (CIPA) of 2000*

The Acceptable Use Policy provides guidelines for all users of the school's information technology resources. Users of any device whether it is of school property or personal property must adhere to the guidelines below. Devices include desktop, laptop or netbook computers, tablets, cell and smart phones, iPods, mp3 players, flash drives, etc. The school's information technology resources, including network resources, email and Internet access, are provided for educational purposes.

**Users shall:**

1. Respect and protect the privacy of others.
  - Use only assigned accounts.
  - Not view, use, or copy passwords to which they are not authorized.
  - Not view or use networks which are not authorized.
  - Not distribute private information about others or themselves.
2. Respect and protect the integrity, availability, and security of all electronic resources.
  - Report security risks or violations to a teacher or network administrator.
  - Not destroy, damage or misuse data, networks, or other resources that do not belong to them, without clear permission of the owner.
  - Conserve, protect, and share these resources with other students and Internet users.
3. Respect and protect the intellectual property of others.
  - Not infringe copyrights (no making illegal copies of music, games, or movies!).
  - Not plagiarize.
4. Respect and practice the principles of community.
  - Communicate only in ways that are kind and respectful.
  - Report threatening or discomfoting materials to a teacher or administrator.
  - Not intentionally access, transmit, copy, or create material that violates the district's code of conduct for students or employees (such as messages that are pornographic, threatening, rude, discriminatory, or meant to harass).
  - Not intentionally access, transmit, copy, or create material that is illegal (such as obscenity, stolen materials, or illegal copies of copyrighted works).
  - Not use the resources to further other acts that are criminal or violate the district's code of conduct for students or employees.
  - Not send spam, chain letters, or other mass unsolicited mailings.
  - Not buy, sell, advertise, or otherwise conduct business, unless approved as a school project.

**Consequences for Violation.** The District may suspend or revoke a user's access to the District's system upon violation of District policy and/or administrative regulations regarding acceptable use.

Students knowingly bringing prohibited materials into the school's electronic environment will be subject to a suspension and/or a revocation of privileges on the District's system and will be subject to disciplinary action in accordance with the Student Code of Conduct.

Employees knowingly bringing prohibited materials into the school's electronic environment will be subject to disciplinary action in accordance with District policies.

**Supervision and Monitoring.** The district monitors the use and security of the information technology resources. Administrators reserve the right to examine, use, and disclose any data found on the school's information networks in order to further the health, safety, discipline, or security of any student or other person, or to protect property. They may also use this information in disciplinary actions, and will furnish evidence of crime to law enforcement.