**SCHOOL DISTRICT OF CAMBRIDGE**

**POLICY # 522.7 Rule**

# PROCEDURES FOR STAFF COMPUTER AND NETWORK USE

1. Privileges

   All hardware and software is the property of the School District of Cambridge. The use of the network is a privilege, not a right, and inappropriate use will result in cancellation of those privileges. If the following procedures are not followed the technology coordinator may temporarily close an account. The administration will then be notified and the user's account may be denied, revoked, or suspended. Appropriate legal action and/or job termination may occur.

2. Acceptable Use

   The use of an account must be in support of education and research and be consistent with the educational objectives of the District. Use of other organizations' network or computing resources must comply with the rules appropriate for that network. The following are prohibited:

   - transmission or duplication of materials in violation of any state or federal law or regulation including, but is not limited to, copyrighted material, threatening or obscene material, or material protected by trade secret;
   - use of computers for personal gain;
   - use of broadcast mail lists for personal solicitation for the buying of, selling of, exchange of, seeking of, or giving of any item or service;
   - use for product advertisement or political lobbying;
   - use related to or in support of illegal activities;
   - use to access, display or print images of a sexual nature;
   - use of the network to harm, harass or discriminate against others (e.g., sending unwanted e-mail, chain e-mail messages, intimidating messages or distasteful messages).

   Any violation of these provisions shall result in disciplinary action and could result in criminal prosecution under state and federal laws and/or job termination. Fines and other costs that result from copyright infringements shall be the responsibility of the user.

3. Network Etiquette

   Users are expected to abide by the generally accepted rules of network etiquette, including, but not limited to, the following:

   - taking responsibility for the ethical and educational use of their own accounts and files;
   - exercising the privilege to use technology as an educational resource by accepting responsibility for all material under his/her account and files;

- using appropriate language and avoiding the use of abusive or offensive language such as swearing or vulgarities; and

- avoiding the disruption of use by others (e.g., downloading excessively large files) since networks are shared resources with limited access time.

4. Personal Use
   Personal use of district computers and the network is permitted during non-contracted time provided that staff members comply with all applicable acceptable use and network etiquette procedures.

5. Ownership and Control
   The District retains ownership and control of its hardware and software at all times. To maintain system integrity, monitor network etiquette and ensure that users are using the system responsibly and legally, school administrators and/or the technology coordinator may review user files and communications. Users shall not expect that files and other information communicated or stored on the District network or servers are private.

6. Security
   Users must notify the technology coordinator of security problems (e.g., known access to in-school network file server or other users' files). All communications, e-mail, file transfers and Web pages visited are not private and will be monitored. Messages relating to or in support of illegal activities must be reported to authorities for possible prosecution under the law.

   Users shall be required to use passwords to access the network and shall not share passwords or use the password of another user. When logged in, staff members shall not allow students to use their computer. Staff members shall not leave the classroom with access to their accounts available.

   Users shall be cautious when downloading files because of the potential for viruses and limitations of the hard drives of the computers and servers. This includes information from the Internet and e-mail. If a staff member is suspicious of a file or e-mail message, he/she should refrain from opening it and contact the technology coordinator. Users may not install software onto the computer hard drives.

   Users are not permitted to access any part of the operating system/hard drive on any networked computer or server.

7. Vandalism
   Vandalism will result in cancellation of privileges and possible legal action. Vandalism is defined as any malicious attempt to harm or destroy hardware, software, and wiring, as well as the data of another user. This includes, but is not limited to, the uploading or creation of computer viruses. Users are financially liable for all vandalism.

---

**LEGAL REFERENCE:**
**CROSS REFERENCE:**
**APPROVED:** February 24, 1997 **REVISED:** July 31, 2000 **POLICY** # 522.7 Rule
WASB Review 9/10
Reviewed: 7/17/17