

# Carver Public Schools Acceptable Use Policy

## Purpose

The Carver Public Schools district provides access to the system/network and the Internet to all employees and students to facilitate communications and access to information in support of educational goals. *Educational goals* are defined as activities that provide for student education, staff professional development, and research. The system/network will also be used for communication with staff, parents and students.

Use of the Carver Public Schools system/network is a privilege, not a right, and must support the stated mission, goals, and objectives of the Carver Public Schools.

A committee of teachers, principals, parents, and students approved the Acceptable Use Policy (AUP). This agreement outlines responsibilities for using the system/network and consequences of abusing that privilege. Every user is required read and sign the AUP before using the Carver Public Schools system/network *each year*. Signing the AUP becomes a legal agreement between the user and the district.

## Terms and Definitions

**AUP:** Acceptable Use Policy

**Chat:** Real-time communication between two users via computer. Once a chat has been initiated, either user can enter text by typing on the keyboard and the entered text will appear on the other user's monitor.

**CPS:** Carver Public Schools

**District:** Carver Public Schools PreK-12

**Electronic Messaging:** chat, email

**Email:** Short for electronic mail, the transmission of messages over communications networks.

**Internet Filter:** Software program or blocker that controls what is shown while a computer user is viewing pages on the World Wide Web.

**System/Network:** Carver Public Schools Network including the Internet, voice mail, email, hardware, software, digital equipment, handheld electronic equipment and individual computer work stations.

**User:** Any student or staff member with an account or anyone else provided access to resources associated with the network.

## User Responsibilities

Use of the network requires individual responsibility. A responsible user:

1. Knows he/she is part of a larger, global community and his/her actions reflect upon him/herself and the school.
2. Does not waste paper and ink, storage space, or bandwidth.
3. Uses time on a workstation or with any other equipment appropriately.
4. Does not share his/her own password.
5. Understands prompt reporting of technical or security problems or inappropriate behavior to a staff member helps all users.

## **Monitored Use**

All messages and information created, accessed, sent, saved, or retrieved on the system/network are the property of the Carver Public Schools and should not be considered confidential. The system/network's backup and filtering mechanism automatically stores communications, including those that have been deleted. The school district reserves the right to access and monitor any messages and information on the system as it deems necessary and appropriate in the ordinary course of business to prevent abuse by network users, to ensure the proper use of resources, and to conduct routine maintenance. Where appropriate, communications, including text, images, or video may be disclosed to law enforcement officials in response to proper requests or to other responsible parties during disciplinary investigation or in the course of litigation without the prior consent of the sender or receiver. Those who use the system/network are considered to have consented to such monitoring and disclosure.

## **Privacy**

In order to protect students' schoolwork, user folders carry individualized security that protects the contents from any other student. Teachers, administrators, and technology staff can access student folders at any time.

There is no expressed or implied level of privacy regarding the contents of user folders or any other use of Carver Public Schools Network and associated resources.

## **Appropriate System/Network Activity**

Activities in support of the District Goals and Objectives that do not violate other school or district policies are acceptable and appropriate. All files stored, viewed, or distributed on the network must be related to schoolwork, including, but not limited to, music, videos, images, URLs, and sound files.

## **Inappropriate System/Network Activity**

1. Intentionally copying, reading, modifying or deleting files or data belonging to another user.
2. Using someone else's password.
3. Pretending to be someone else when using the system/network.
4. Deliberate attempts to degrade or disrupt system performance including vandalism or theft of hardware, software applications, files, or system configurations, attempting to introduce viruses, malicious code, or any other violation of district policy, state, or federal law.
5. Intentionally bypassing or attempting to bypass CPS security, including attempts to bypass Internet filtering.
6. Installing software or programs that have not been approved by the technology department.
7. Revealing personal information about others on the Internet.
8. Revealing personal information about yourself on the Internet without the expressed permission of a supervising staff member and parent or guardian.
9. Intentional storage, viewing, or distribution of any text, video, audio, images, or graphics considered inappropriate within a school environment. Inappropriate materials include, but are not limited to, those containing content that is profane or obscene, racial or ethnic slurs, vulgar, sexually explicit, threatening, defamatory, abusive, discriminatory, harassing, criminal or otherwise objectionable or that depicts, suggests or implies illegal activity, drug

use or gambling, shows or encourages violence against a living being or physical property, provocative or explicit dress or undress.

10. Violating the legal protection of copyright, including the use of materials or ideas without properly citing their sources. This includes copying or downloading music, software, games, or any proprietary materials covered by copyright law.
11. Activities designed to harass other users.
12. Advertising or advocating for non-school related activities or for-profit organizations, campaigning for political office, or “chain letters.”
13. Use of the system/network for commercial transactions that benefit an individual or group.
14. “Chats” and games unless approved, directed, and supervised by an appropriate member of the school faculty or administration. The Director of Technology must expressly approve the storage, installation, and use of such files or applications.

### **Consequences**

In cases where it has been determined that a user has acted inappropriately, the administrative staff, in consultation with the Director of Technology, may take the following actions against the user:

1. File documentation with an administrator for investigation.
2. Restrict network access pending investigation.
3. Confiscation of personal equipment including laptops, software, cell phones, and other electronic devices.
4. Suspend or deny user account and privileges to CPS System/Network and all associated resources.
5. Implement disciplinary action up to and including suspension or expulsion.
6. Pursue legal action, including criminal prosecution, as appropriate under local, state, and federal law.

### **Liability**

Carver Public Schools is in compliance with the Children’s Online Privacy Protection Act (COPPA) and Children’s Internet Protection Act (CIPA). As required by law, the school district has in place an Internet filtering mechanism that protects minors from unlawful, obscene, or harmful material.

### **Disclaimer**

Access to information all over the world via computer brings with it an availability of material that may not be considered educationally valuable. It is impossible to control access to all materials and a user may unintentionally discover controversial or objectionable information. CPS policy affirms that the educational value of access to information and the potential for interaction on the Internet far outweighs the possibility that users may be exposed to materials not consistent with the educational goals of the district. CPS makes no warranties of any kind for the service it provides. The town of Carver, the School Department, or any municipal employees will not be liable for damages or injuries resulting from violations of the Acceptable Use Policy or any misuse of the Internet.