



The Colorado Springs School - Acceptable Use Policy

1.0 Overview

The intention of publishing an Acceptable Use Policy is not to impose restrictions that are contrary to The Colorado Springs School's established culture of openness, trust, and integrity. The Colorado Springs School is committed to protecting the employees, students and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. Internet systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, internet browsing, and File Transfer Protocols are the property of The Colorado Springs School. These systems are to be used for business purposes in serving the interests of the agency in the course of normal operations. Effective security is a team effort involving the participation and support of every Colorado Springs School employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines and to conduct their activities accordingly.

2.0 Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at The Colorado Springs School. These rules are in place to protect the employees, students, and The Colorado Springs School. Inappropriate use exposes The Colorado Springs School to risk including virus attacks, compromises of the network systems and services, and legal issues.

3.0 Scope

This policy applies to anyone accessing The Colorado Springs School network.

4.0 Policy

4.1 General Use and Ownership

1. While The Colorado Springs School's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the



corporate systems remains the property of The Colorado Springs School. Because of the need to protect The Colorado Springs School's network, management cannot guarantee the confidentiality of information stored on any network device belonging to The Colorado Springs School.

2. For security and network maintenance purposes, authorized individuals within The Colorado Springs School may monitor equipment, systems and network traffic at any time, per The Colorado Springs School's policy.
3. The Colorado Springs School reserves the right to audit the network and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

1. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts.
2. All personal computers, laptops, and workstations, and/or any device on the network should be locked to prevent inadvertent viewing when a device is unattended.
3. Because information contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops in accordance with policy.
4. All devices used by employees that are connected to The Colorado Springs School network, whether owned by the employee or CSS, shall be continually executing virus-scanning software with a current database.
5. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

4.3 Unacceptable Use

The following activities are, in general, prohibited. Under no circumstances is an employee of The Colorado Springs School authorized to engage in any activity that is illegal under local, state, federal, or international law utilizing The Colorado Springs School owned



resources. The list below is by no means exhaustive but attempts to provide a framework for activities which fall into the category of unacceptable use.

The following activities are strictly prohibited, with no exceptions:

1. Unauthorized access, copying, or dissemination of sensitive information.
2. Installation of any copyrighted software for which The Colorado Springs School or end user does not have an active license is strictly prohibited.
3. Installation of any software on devices owned by CSS without preapproval is strictly prohibited.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, logic bombs, etc.).
5. Revealing your account password to others or allowing use of your account by others.
6. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For the purpose of this policy, “disruption” includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
7. Port scanning or security scanning is expressly prohibited unless prior notification has been given to The Colorado Springs School.
8. Executing any form of network monitoring that will intercept data not intended for the employee’s host, unless this activity is a part of the employee’s normal job/duty.
9. Circumventing user authentication or security of any host, network, or account.
10. Interfering with or denying service to any user other than the employee’s host.