Centinela Valley Union High School District

Educational Services Division

14901 S. Inglewood Avenue
Lawndale, CA 90260
www.centinela.k12.ca.us

Acceptable Use Policy for District Computer Systems

Information for Employees, Students, and their Parents/Guardians

This Acceptable Use Policy was adopted by the Board on May 13, 2014.

The goal of Centinela Valley Union High School District's (the"District") Acceptable Use Policy ("POLICY") is to prevent unauthorized access and other unlawful activities by Users online, prevent unauthorized disclosure of or access to sensitive information, and to comply with the Children's Internet Protection Act ("CIPA"). As used in this POLICY, "Network" includes all internet and intranet services and connections (including but not limited to email, web services, and all forms of electronic communication), software, websites, web-based programs, services and content, hardware, and all technology equipment and peripherals, including but not limited to computers, tablets and other devices provided by the District. As used in this policy, "User" includes anyone using the Network. **Only current students or employees are authorized Users of the Network.** This POLICY covers all connections to and use of the District Network by any device (regardless of ownership and/or location of that device), and District-owned hardware (including but not limited to computers and tablets) at all times, even when that hardware is not on district property.

To the extent practicable, the District will use commercially reasonable measures to block or filter visual depictions that are *obscene, pornographic, and harmful to minors* over the Network. The District reserves the right to monitor Users' online activities and to access, review, copy, and store or delete any electronic communication or files and disclose them to others as it deems necessary.

Users should have no expectation of privacy when using the Network. The District can and does monitor Internet access and activity on the Network, including but not limited to sites visited, content viewed and email sent and received. The District may examine a User's personal device and search its contents if there is a reason to believe that school policies, regulations, or guidelines regarding access to the Network or use of the device have been violated.

The District will take all necessary measures to fortify the Network against potential cyber security threats. This may include blocking access to District applications—including but not limited to email, data management and reporting tools, and other web applications outside the United States and Canada.

Acceptable Uses of the Network

Schools must verify each year that all employees and students using the Network for that school year have acknowledged this POLICY via an executed acknowledgement page. Students who are under 18 years of age must have their parents or guardians sign the acknowledgement page and schools must keep the executed acknowledgement page for each employee and student on file. Once signed, the acknowledgement page remains in effect until revoked by the employee or parent/guardian, or the student is no longer a District student. Employees, students and other Users are required to adhere to the requirements of this POLICY. **By virtue of using the Network, Users are agreeing to follow this POLICY** and report any misuse of the Network to a teacher, supervisor or other appropriate District personnel. Access is provided primarily for education and District business. Employees may use the Network for incidental personal use during duty-free time**.** If a User is uncertain about whether a particular use is acceptable or appropriate, he or she should consult a teacher, supervisor or other appropriate District personnel.

Unacceptable Uses of the Network

The District reserves the right to take immediate action regarding activities (1) that create security and/or safety issues for the District, students, employees, schools, Network or computer resources, (2) that expend District resources on content the District in its sole discretion determines is in violation of applicable laws or lacks legitimate educational content/purpose, or (3) other activities determined by District as inappropriate. The following are examples of inappropriate activity on the Network:

1) **Violating any state or federal law or municipal ordinance, such as: Accessing or transmitting pornography of any kind, obscene depictions, harmful materials, materials that encourage others to violate the law, misusing confidential information or copyrighted materials;**
2) **Undertaking criminal activities that can be punished under law;**
3) **Selling or purchasing illegal items or substances;**
4) **Obtaining and/or using anonymous email sites;**

Continues on next page

5) **Spamming;**

6) **Spreading viruses;**
7) **Online gaming (e.g., World of Warcraft) unless approved by a teacher;**
8) **Downloading software, music, movies or other content in violation of licensing requirements, copyright or other intellectual property rights;**
9) **Using proxy sites;**
10) **Unauthorized remote access to the Network;**
11) **Cheating/plagiarism;**
12) **Cyberbullying;**
13) **Causing harm to others or damage to their property, such as:**
    a) Using profane, abusive, or impolite language; threatening, harassing, or making damaging or false statements about others or accessing, transmitting, or downloading offensive, harassing, or disparaging materials;
    b) Deleting, copying, modifying, or forging other people's names, emails, files, or data; disguising one's identity, impersonating other people, or sending anonymous email;
    c) Damaging computer equipment, files, data or the Network in any way, including intentionally accessing, transmitting or downloading computer viruses or other harmful files or programs, or disrupting any computer system performance;
    d) Using any District computer to pursue "hacking," internal or external to the District, or attempting to access information protected by privacy laws; or
    e) Accessing, transmitting or downloading large files, including "chain letters" or any type of "pyramid schemes".

14) **Engaging in uses that jeopardize access or lead to unauthorized access to others' accounts or other computer networks, such as:**
    a) Using another's account password(s) or identifier(s);
    b) Interfering with other Users' ability to access their account(s); or
    c) Disclosing anyone's password to others or allowing them to use another's account(s);
    d) Using another's account to access confidential information and/or alter student, school or District records.

15) **Using the Network for Commercial purposes:**
    a) Using the Internet for personal advertising, promotion, or financial gain; or
    b) Conducting for-profit business activities and/or engaging in non-government related fundraising or public relations activities such as solicitation for religious purposes, or lobbying for personal or political purposes.

Student Internet Safety

1) Students under the age of eighteen should only access District accounts outside of school if a parent or legal guardian supervises their usage at all times. The student's parent or guardian is responsible for monitoring the minor's use;
2) Students shall not reveal personal information about themselves or other persons. For example, students should not reveal their name, home address, telephone number, or display photographs of themselves or others;
3) Students shall not meet in person anyone they have met only on the Internet; and
4) Students must abide by all applicable laws, this POLICY and all District security policies.

Penalties for Improper Use

The use of a District account to access the Network is a privilege, not a right, and misuse will result in the restriction or revocation of privileges to use the Network. Misuse may also lead to disciplinary and/or legal action for both students and employees, including suspension, expulsion, dismissal from District employment, or criminal prosecution by government authorities. The District will attempt to tailor any disciplinary action to the specific issues related to each violation. Users may be held liable for any damage to the Network, including but not limited to damages to technology equipment and/or damages caused as a result of using the District Network.

Disclaimer

The District makes no guarantees about the quality of the services provided and is not responsible for any claims, losses, damages, costs, or other obligations arising from use of the Network or related accounts. Any charges a User accrues due to the use of the District's Network are to be borne by the User. The District also denies any responsibility for the accuracy or quality of the information obtained through the Network. Any statement, accessible on the Network, is understood to be the author's individual point of view and not that of the District, its affiliates, or employees.

14901 S. Inglewood Avenue
Lawndale, CA 90260
www.centinela.k12.ca.us

Acceptable Use Policy for District Computer Systems
Acknowledgement by Employees, Students, and their Parent/Guardians

I have read, understand, and agree to abide by the provisions of the Acceptable Use Policy of the Centinela Valley Union High School District.

This agreement is for a (check the appropriate box):
☐ **Student** ☐ **Employee**

School: _____ **Date:** _____

Employee or Student Name: _____

Employee or Student Signature: _____

If the student is under 18 years of age, a Parent or Legal Guardian Signature is required below

Parent/Legal Guardian Name: _____

Parent/Legal Guardian Signature: _____

Return this form to the school where it will be kept on file.
It is required for all employees and students that will be using the the District's Network.