

NOVATO UNIFIED SCHOOL DISTRICT

TECHNOLOGY AND ELECTRONIC SERVICES POLICY FOR EMPLOYEES AND SUBSTITUTES

Purpose

The Novato Unified School District (“District”) provides its employees and substitutes (jointly, “employees”) with access to Electronic Services including email systems, network connections, Internet, mobile communications devices, and District social media accounts (podcasts, blogs, and Youtube). This policy governs employee access to and use of the District’s Electronic Services.

Privacy/Inspection

Employees do not have an expectation of privacy in using the Electronic Services. The District routinely monitors its Electronic Services without advance notice or consent, and information stored on or transmitted by the Electronic Services is the property of the District. Employees shall not remove any information stored on the Electronic Services

Acceptable Use

Employees shall use the Electronic Services for District business consistent with its educational mission.

Employees may use the Electronic Services for protected union activity during non-duty hours provided that such use does not interrupt District business

Employees may use the Electronic Services for personal business only during non-duty time and out of view of the public, provided such use does not interfere with District business. The District may revoke or limit this privilege without advance notice.

Employees may use their personal cellular phones or mobile communication devices for personal business during off-duty time and out of view of the public.

In an emergency, employees may use the Electronic Services or personal communications devices as needed.

The District will determine the existence of an emergency on a case-by-case basis.

Unacceptable Use

An employee may not transmit material in violation of Board Policy, Administrative Regulation, or federal and state law.

Employees may not access or disclose confidential information (any information that is not subject to public disclosure), discriminate against or harass another based on his or her membership in a legally protected class, view obscene or violent material, download unauthorized software, infringe upon copyrighted or trademark information, conduct commercial activities, advertise products for profit, or engage in political lobbyist activities.

Professional Standards

Employees must observe common professional standards when accessing and using the Electronic Services. An employee must comply with state and federal laws, Board Policies and Administrative Regulations, and the applicable collective bargaining agreement.

Employees are also expected to use appropriate language, secure confidential information, be polite and respectful, not disrupt or interfere with District business, and not discuss personal business.

Email

The District provides employees with access to the District's email accounts to conduct District business. Employees shall not conduct District business on their personal email accounts.

The District's email account may be subject to disclosure pursuant to public disclosure laws; therefore, employees must observe professional standard when sending and receiving emails.

Internet Access

Employees are provided with access to the Internet to conduct District business. Employees shall not disable the District's internet filters to access prohibited websites without written consent from his or her department supervisor. The District may revoke an employee's internet privileges for unacceptable use and impose appropriate discipline.

District Network

The District provides employees with a login ID and password to access the District's network. The network contains confidential District information; therefore, employees shall not disclose their login ID or password to anyone, except his or her supervisor if necessary.

If an employee suspects that his or her ID or password has been compromised, the employee must immediately notify his or her supervisor and the Information Technology Department. Employees may be responsible for the consequences occurring under their login or password due to any neglect on their part.

Professional Social Media

Employees shall not create professional social media web pages pertaining to District business without prior written consent of his or her immediate supervisor and the District's legal counsel. All District social media web pages must be maintained according to District Policies and Administrative Regulations and state and federal laws. Employees must obtain written permission from his or her department supervisor to post proposed comments or images on the District's social media web page.

Personal Social Media

This policy does not govern employees' use of personal social media. However, the District encourages employees to exercise caution when accessing and using personal social media. Employees should not post or include any references to the District on their personal social media web pages. Employees are encouraged to include disclaimers on their personal social media web pages indicating that the views and comment expressed therein do not represent those of the District. Employees should not post or advertise any District related event without prior written consent from the department supervisor. Employees should refrain from posting any image associating oneself with any perceived or actual illegal activity because he or she may be subject to discipline pursuant to applicable state and federal laws, Board Policies and Administrative Regulations, or collective bargaining agreement provisions.

Security

The District does not expressly or impliedly warrant employees's use of its Electronic Services.

Vandalism

Employees shall not vandalize the District's Electronic Services. Vandalism is defined as any malicious attempt to harm, destroy or misrepresent data of another user, agency, or other

networks that are connected. Employees shall not upload or create computer viruses or any program intended to disrupt the Electronic Services.

Discipline

Employees are subject to discipline for violation of this policy, consistent with the relevant collective bargaining agreement, Board Policies and Administrative Regulations, or state and federal law.

Personal Responsibility

As an employee of the District, I will report any misuse of the Electronic Services to the systems administrator, including any conduct prohibited by this policy.

I read this policy and understand my personal and professional responsibilities with regard to using the District's Electronic Services

User's Full Legal Name (PLEASE PRINT)

Date

Position

Work Location

User's Signature