La Vernia ISD Employee Acceptable Use Policy

Introduction

La Vernia ISD incorporates technology as a natural part of education and administration. The use of technology empowers employees and promotes life-long learning through access to the latest equipment, information and resources.

Computers and technology are integrated into every facet of the educational and administrative process. La Vernia ISD endeavors to provide appropriate educational technology and the skills required to use this technology responsibly for all employees in order to prepare them for the classroom and workplace of tomorrow.

La Vernia ISD's technology includes campus-wide and District-wide computer networks utilizing direct Internet access and Cloud-based resources. Distance learning, streaming web-based video content, electronic mail and fax services are also available.

Personal Devices, Remote Access and Virtual Presence

This policy applies to and governs **all** use of technology at **all** times when an employee is on District property, whether the employee is using District-provided technology devices or their own personal electronic devices. La Vernia ISD also provides remote access to District technology resources and tools including virtual desktop environments which are accessible from anywhere in the world via the Internet. If an employee is accessing a District-provided virtual desktop environment via the Internet from a remote location, *the connection constitutes a virtual presence on District property*, and all District policies and regulations apply to the employee and are enforced as if the employee were physically present on District property.

Internet Safety

Secure access firewalls and content-filtering software are utilized in order to protect employees and students from inappropriate content on the Internet/World-Wide Web and to comply with protective laws and regulations including CIPA, the Children's Internet Protection Act. The school district will educate all students and staff about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, disclosure of the personal information of minors, and cyberbullying awareness and response.

The La Vernia ISD Employee Acceptable Use Policy explains and defines responsible and ethical use of technology for all employees. All rules embodied herein guide employees in appropriate and acceptable use of District technology, and are designed to protect both the employee and the District. This policy also governs the use of employee-owned personal electronic devices including wired or wireless desktop, portable and handheld technology tools including computing and gaming devices, cameras, and cellular telephones.

Acknowledging Conformance to Acceptable Use Policy

Access to technology and electronic communication systems, including computer networks and the Internet, is made available exclusively for instructional and administrative purposes in accordance with District guidelines and regulations. **Access to these systems is a privilege, not a right**.

All employees are required to acknowledge receipt and understanding of the Employee Acceptable Use Policy document and must agree in writing to comply with all regulations and guidelines contained herein.

Employees will not be allowed access to any technology or computer equipment in La Vernia ISD until their Employee Acceptable Use Policy Authorization Form has been signed and returned to their administrator.

Once their authorization form has been returned, each employee will be issued a unique login identification code allowing access to the appropriate information systems. Employees must maintain a secure and confidential password.

All passwords are confidential and must not be revealed to other employees or students.

Employees with questions or concerns regarding the Employee Acceptable Use Policy should contact their administrator or call the La Vernia ISD Technology Department at (830) 779-6610.

Employee Acceptable Use Policy

La Vernia ISD declares the following unethical and unacceptable behavior just cause for taking disciplinary action, suspending or revoking access privileges, suspending or terminating the employee, and/or initiating legal action in any case in which the employee:

- Uses the network and/or any equipment, whether owned by the District or the employee, for illegal, inappropriate, subversive or obscene purposes or activities. Illegal activities shall be defined as activities violating local, state and/or federal laws, including use of the network to commit forgery, fraud or assist in the commission of a felony. Inappropriate use shall be defined as a violation of the intended educational or administrative use of the network. Subversive activities shall be defined as activities undermining the security of local, state or national governments, or activities intended to cause mental anguish, bodily injury or death to any citizen or group of citizens, including “cyber-bullying” and “flaming” (flaming is a hostile and insulting interaction between Internet users, typically via email or messaging forums). Obscene activities shall be defined as a violation of generally accepted social standards for use of a publicly-owned and operated communications vehicle, including possession or transmission of any form of pornographic or erotic material;
- Uses the network and/or any equipment, whether owned by the District or the employee, for any illicit activity, including violation of copyrights, patents, institutional or third-party copyrights, license agreements or other contracts, whether the activity is conducted via the public Internet, private intranet or through peer-to-peer file sharing. Illicit activities also include transmitting or accessing information designed to aide or abet an individual or group in violating the law, including all forms of access to gang-related, terrorist-related or organized-crime-related web sites, weblogs and bulletin boards;
- Uses the network and/or any equipment, whether owned by the District or the employee, to obtain and/or distribute illegally (“traffic”) via the public Internet, private intranet or through peer-to-peer file sharing any and all digital music, video, movie and/or software from copyrighted sources. This expressly prohibits accessing, executing or installing Internet and/or peer-to-peer file sharing software for the sole purpose of accessing or disseminating non-public-domain content and prohibits accessing websites and web rings designed to traffic or disseminate non-public-domain content and entertainment including, but not limited to, MP3 audio files, videos, movies, and executable software code;
- Intentionally disrupts network traffic, deliberately “crashes” the network or connected systems or tampers with communications cabling and/or devices;
- Damages or destroys computer and/or network equipment or deliberately degrades system performance, including executing “Denial of Service” or similar attack code and/or infection of computers or servers with viruses or malware;
- Discloses his/her password to another employee or attempts to disclose or discover another employee’s password;

- Attempts to copy District-owned software for personal gain, attempts unauthorized transport of District-owned software beyond District boundaries, attempts to install privately-owned software onto a computer or the network or transmits any non-public-domain software via electronic mail or the Internet;
- Downloads, transfers, accesses or otherwise installs programs and/or executable code or files onto any computing device without appropriate permission and supervision;
- Uses La Vernia ISD network or computer resources for commercial or financial gain;
- Steals or vandalizes data, equipment or intellectual property;
- Gains or attempts to gain unauthorized access to internal and external resources or entities, including “hacking” into networks, web sites, private electronic mail accounts, weblogs (blogs) or bulletin boards;
- Gains or attempts to gain unauthorized access to external resources or entities via use of Internet proxy sites and/or proxy servers designed to bypass District monitoring, security and content filtering devices;
- Forges or alters electronic mail messages or faxes, posts anonymous messages, acts as a “troll” (lurking anonymously on message boards for the purpose of disparaging other users), engages in “flaming” (flaming is a hostile and insulting interaction between Internet users, typically via email or messaging forums), deliberately propagates spam or uses an account or password owned by another user;
- Invades or assists others in invading the privacy of an individual or group, including cyberbullying and the use or deployment of any form of virus/worm, Trojan (a program appearing to be beneficial while serving as a delivery vehicle for malicious content), identity theft or phishing (gaining personal information through nefarious means) executable code or software;
- Possesses or conveys any data in any form including magnetic (disk/tape/ memory device), optical (CD-ROM) or hardcopy (paper) which might be considered a violation of these rules.

Once logged into the system, employees will be held accountable for all activities and data transfers occurring on their computer. Any illegal or illicit use will be tracked to the employee logged in. Employees will be held accountable for their computer whether they or another employee or student initiate the activity and must not let other employees or students access their computer. **Employees must properly log off the system before leaving their computer.**

Limited Personal Use of District systems is permitted; Limited Personal Use includes actions such as checking private email accounts and accessing non-work-related web sites during breaks *provided the content complies with AUP guidelines* and *provided this access does not interfere with the performance of assigned duties*.

Usage of Personal Electronic Devices:

Employees are restricted in their usage of employee-owned personal electronic devices on District property and at District-sponsored events. Personal electronic devices include but are not limited to employee-owned desktop, laptop, tablet and handheld computing devices, whether wired or wireless, USB drives, cameras and cellular telephones.

The following activities are regulated by the Acceptable Use Policy:

- Employees are prohibited from using mobile and portable technology tools "smartphone" device (combination cellular phone including handheld computer and web browser functionality), traditional cellular phones or a camera phone (a cellular phone including a camera capable of capturing and transmitting still or full motion images) in any way that violates School or District policies, including illicit and illegal use.
- Employees are prohibited from using **any** cabled, USB or wireless (Wi-Fi) IP phone device, such as the Vonage V-Phone or MagicJack, on the District network.
- Employees are prohibited from using **any** wearable, automated life-logging or live-video-blogging cameras, such as Memoto or GoPro, at any time without prior written permission from District administration. Such written permission, if granted, must specify the circumstances, times and situations during which any such camera may be enabled.
- Employees are prohibited from using **any** augmented reality devices, such as Vuforia or Google Glass, at any time without prior written permission from District administration. Such written permission, if granted, must specify the circumstances, times and situations during which any such device may be enabled, and must further specify the circumstances, if any, during which any video recording capabilities may be enabled.
- Employees are prohibited from using film or digital cameras and film or digital camcorders in any way that violates School or District policies, including illicit and illegal use.
- Employees are prohibited from using any handheld media player device (such as an iPod) or any portable handheld computing or gaming device (similar to a PSP) in any way that violates School or District policies, including illicit and illegal use.
- Employees may not use any personal electronic devices or media including but not limited to CD/DVD burners and USB "pen" or "jump" drives (USB keys), or web-based/Cloud-based file sharing sites to illegally duplicate and/or distribute copyrighted materials including music, video, movies and software.
- Employees may not load a bootable, alternate operating system on any District-owned computer or attempt to boot a District computer directly from any employee-owned source or media, including floppy disks, CD/DVD discs or USB devices ("pen" or "jump" drives, USB keys, USB hard drives or USB CD/DVD drives).

Violations of these policies will result in the immediate confiscation of the involved device(s) or media as appropriate. Depending upon the nature and severity of the violation, the confiscated device(s) or media may be held in evidence indefinitely.

Disclaimer

The District shall not be liable for any employee's inappropriate use of electronic communication resources, violations of copyright restrictions, users' mistakes or negligence or costs incurred by employees. The District shall not be responsible for ensuring the accuracy or usability of any information found on the Internet/World-Wide Web.

The District attempts to block, restrict, impede, or otherwise seeks to limit employee access to web sites known to distribute file-trafficking software. Reasonable attempts are made to monitor employee content maintained on District systems. It is the policy of La Vernia ISD to disclose information to the extent allowed by law when responding to notices of infringement received from copyright holders.

Electronic mail transmissions, faxes, and program or data files sent, received, created or accessed by employees are not considered confidential and may be monitored at any time by District staff to insure appropriate use of the educational technology.

La Vernia ISD has the right to restrict or terminate Internet, network or computer access at any time for any reason. The District also has the right to monitor Internet, network and computer activity in any way necessary to maintain the integrity and security of the network and the privacy and accuracy of user information.

Consequences of Violations of the Employee Acceptable Use Policy

Consequences of violations include but are not limited to:

- Suspension or revocation of Internet access privileges
- Suspension or revocation of electronic mail and/or fax privileges
- Suspension or revocation of network access privileges
- Suspension or revocation of computer access privileges
- Any and all consequences defined in the Employee Handbook and/or District and Board policies, including:
- Suspension with or without pay;
- Termination; and
- Legal action and/or prosecution by the authorities.

Remedies and Recourse

Employees accused of violating the Employee Acceptable Use Policy have full rights to due process and appeals as set forth in District Policy.