La Mesa-Spring Valley School District
Employee Technology Responsible Use Policy

The Employee Technology Responsible Use Policy ("Policy") applies to all La Mesa-Spring Valley School District ("District") employees and any other person or entity granted access to or use of District computers, tablets, cell phones, software applications, e-mail, and Internet network (collectively, "Technology"), whether or not employed by the District ("Users"). To gain access to District Technology, Users must review and abide by the terms of this Policy and District policies.

1. Educational and Business Objectives

- District Technology is intended for District business and educational purposes.

2. Property

- All Technology is owned by the District. All files stored on Technology are considered to be property of the District, and materials developed by District staff in the course of carrying out their professional responsibilities on District time shall be the property of District.
- All Technology and business files must be returned immediately upon termination of District employment.
- Neither the hardware nor software configuration can be changed without specific permission from the Information Systems Department. Examples of changes requiring authorization include: installing new software or hardware, formatting a hard drive, adding new drivers. To request a change, submit a Service Request to the Information Systems Department. Any intentional damage to the configuration of Technology may result in discipline.
- User is responsible for taking reasonable steps to keep LMSVNET password confidential. The password cannot be given to students or anyone who is not a District employee. Guest passwords are available upon request from the Information Systems Department.
- Personal devices are not allowed on the District network without permission of the Information Systems Department.
- If Technology issued to a User is stolen, whether on District or private property, the User is responsible to immediately notify the police and a copy of the report must be submitted to the Business Office.
- All desired Technology repairs must be reported the District Work Order System and repaired only by personnel authorized by the District.

3. Email

- District employees must exclusively use their District-provided email account (@lmsvsd.net) for email correspondence related to District business or student/educational information.

4. No Expectation of Privacy

- USERS OF DISTRICT TECHNOLOGY (INCLUDING BUT NOT LIMITED TO EMAIL AND THE INTERNET) HAVE NO EXPECTATION OF PRIVACY.
- Any or all uses of Technology may be intercepted, recorded, monitored, copied, deleted, audited, inspected and disclosed to authorized personnel as well as any other person or entity permitted access under the law.
- District shall cooperate with law enforcement agencies investigating illegal activity on the District Technology.

5. User Back-up

- District may conduct nightly network back-ups. Users with District Technology are responsible for copying critical work-related business and data files onto the network for regularly scheduled back-up.

- Personal data files should not be stored on the District network. Users should back up such files on personally owned local drives.

6. **Internet Service Providers**
    - While on a District site, staff must access the Internet on Technology only through the District network. All Internet traffic must pass through the District network where access controls and related security mechanisms will be applied.
    - Staff must not bypass the District network, security mechanism, or content filtering policies. Staff may receive a filter bypass code from a District Manager upon request, and use it with prior approval from the District Manager. The filter bypass code shall not be shared with students or anyone who is not an employee of the District.

7. **Safety**
    - Sharing of personal information via the internet such as name, address, and phone number, can compromise personal safety. Privacy cannot be guaranteed in a network environment.

8. **Confidentiality of Information**
    - District staff may have access to information that is confidential. District requires that staff take reasonable measures to maintain absolute confidentiality in all electronic student, employee, and application matters.
    - Access to confidential information REGARDING DISTRICT STAFF OR STUDENTS is authorized ONLY when staff have a legitimate District need to access the information, and for which they have explicit authorization.
    - UNAUTHORIZED ACCESS TO OR DISSEMINATION OF CONFIDENTIAL INFORMATION SHALL BE GROUNDS FOR DISCIPLINE UP TO AND INCLUDING TERMINATION.
    - Failure to take reasonable steps to secure sensitive information shall be grounds for discipline, including possible termination.

9. **Liability**
    - The District makes no assurances of any kind, expressed or implied, regarding any Technology.

10. **Appropriateness of Materials**
    - Access to the Internet provides opportunities for staff and students to explore resources outside their schools or offices. The District acknowledges obscene materials exist and will make reasonable efforts to avoid obscene materials, including the use of filtering software. However, no software or appliance can filter out all materials that are obscene and all staff, students, and students' parents/guardians understand that intentional access to obscene material is strictly forbidden. Any violation may be cause for restriction or discipline, up to and including termination.
    - If staff or a student unintentionally accesses obscene information while doing legitimate research, he/she should contact the person responsible for technology at his/her site.
    - It is the responsibility of all staff and students, to ensure that District Technology is being used for educational or District business purposes.

11. **Copyright**
    - Unless it is otherwise stated, Users should assume that all materials on the Internet, including web sites and pictures, are copyrighted. Existing copyright guidelines apply, such as those involving photocopying and fair use. Copyrighted material shall be posted online only in accordance with applicable copyright laws.

- Staff or students must not copy software on any District Technology and may not bring software from outside sources for use on District Technology without the prior approval of the Information Systems Department or its designee.
- The District shall not be responsible or liable for unauthorized use or distribution of copyrighted materials and reserves the right to seek indemnification from the User for the inappropriate use, distribution or possession of copyrighted material on the District Technology.

12. User Accounts and Passwords

- A User in whose name a District account is issued is responsible at all times for its proper use, and such User shall access the system only under the account assigned.
- Passwords must never be shared. Sharing a User ID or password exposes the User to responsibility for actions others take with the password or ID.
- Users must take reasonable steps to ensure the security/privacy of their passwords, including changing the password periodically, selecting a password that is reasonably complex and known only to the User, and never displaying the password in a public place.

13. Security

- Users may not prepare, alter or complete the installation of any physical or logical connection to the Technology. This includes connecting computers, servers, network electronics or other network enabled devices to the District Technology, such as multicomputer file systems, web services, internet, and FTP servers.
- Users may not establish any unauthorized server or file sharing mechanism, including, but not limited to, intranet servers, electronic bulletin boards, instant messaging, local area networks, modem connections to existing networks, or multi-user systems for communicating information.
- No proxies or personal firewalls are allowed.

14. Use of Wireless Devices

- Tablets, cellular phones, and other wireless devices may contain sensitive information and must be secured in the same manner as computers, such as using a password, etc. These devices will be issued and returned according to District equipment procedures.

15. Appropriate Behavior

- Staff members are responsible for appropriate behavior on the District Technology, and must adhere to all relevant federal, state, and local laws, as well as District policies and procedures.

16. Staff Working with Students

- Employees working with students are responsible for supervising use of District Technology and enforcing this Policy at all times while working with the students.

17. Consequences of Violation – Disciplinary Action

- A violation of this Policy may be cause for discipline, up to and including termination.
- If a User is accused of a violation, he/she has all of the rights and privileges that a User would have if he/she were subject to any other type of disciplinary action.
- Users assume personal responsibility and liability, both civil and criminal, for uses of the Technology not authorized by this Policy and any District guidelines.
- The District does not sanction any use of its Technology that is not authorized by or conducted in strict compliance with this Policy.

  The District retains the right to remove from its Technology any material it views as obscene, offensive, unrelated to the purpose of the website, or potentially illegal, in accordance with the law.

(BP/AR 4040 Employee Use of Technology)

PLEASE SIGN BELOW:

- I have read, understand, and will follow the rules in this Policy. I understand that if I violate this Policy, I may face disciplinary measures, including termination. Failure to sign does not absolve Users from the responsibility to comply with this Policy.
- I understand that Internet sites are filtered and that any District Technology use may be monitored by the District.
- I release the District, its personnel and any institutions with which it is affiliated, from any and all claims and damages of any nature arising from my use of, or inability to use, the District Technology, including but not limited to claims that may arise from the unauthorized use of the system.
- I have read and understand the attached two-paged Social Media Guidelines.
- Staff working with students: I agree to enforce this Policy with students under my supervision.

Employee Name ______________________________ Employee ID ____________________

Signature ____________________________________ Date Signed ____________________

Current Work Location ____

Social Media Guidelines

Although staff members enjoy free speech rights guaranteed by the First Amendment to the U.S. Constitution, certain types of communication, typically by virtue of their subject-matter connection to campus, may relate enough to school to have ramifications for the author or subject at a District site.

When using District technology, electronic communication is governed by the Employee Technology Responsible Use Policy, which will be enforced accordingly. Staff should not expect privacy in the contents of their personal files on the District's Internet system or other District technology, including email.

Use of personal technology or devices may also violate the District's policy if the District reasonably believes the conduct or speech will cause actual, material disruption of school activities or a staff member's ability to perform his or her job duties.

Off-campus internet usage is largely unrelated to school; however, in certain circumstances courts have held that the off-campus online communications may be connected enough to campus to result in either student or staff-member discipline.

These guidelines are intended to present to District staff members examples of such situations, and guidelines for responsible, ethical internet use.

1. **Limit On-Duty Use** – Staff members must limit their personal technology use during duty hours. Personal use of technology for non-District business should be limited to off-duty time and designated breaks.

2. **Work/Personal Distinction** – Staff members are encouraged to separate their personal social media use and any District-related social media sites.

3. **Student Photographs** – Absent parent permission, staff members must not send, share, or post pictures, text messages, e-mails or other material that personally-identifies District students.

4. **Professional Effectiveness** – District employees must be mindful that any Internet information is ultimately accessible to the world. To avoid jeopardizing their professional effectiveness, employees are encouraged to familiarize themselves with the privacy policies, settings, and protections on any social networking websites to which they choose to subscribe and be aware that information posted online, despite privacy protections is easily and often reported to administrators or exposed to District students.

5. **Personal Social Networking & Media Accounts** – Before employees create an account or join an online social network, they should ask themselves whether they would be comfortable if a 'friend' decided to send the information to their students, the students' parents, or their supervisor. Educators must give serious thought to the implications of joining an online social network. District employees should use appropriate discretion when using social networks for personal communications and should limit this activity to personal devices.

6. **Responsible Online Identity Monitoring** – Employees are encouraged to monitor their 'online identity,' by performing search engine research on a routine basis in order to prevent their online profiles from being fraudulently compromised or simply to track information posted about them online. If there is unwanted information posted about the employee online, the employee may be able to contact the site administrator to request removal.

7. **Friending District Students** – Employees are encouraged to limit online interactions with students on social networking sites outside of forums dedicated to academic use.

8. **Contacting Students Off-Hours** – When contacting a District student during off-duty hours, it is recommended that staff begin by contacting the student's parent(s) or legal guardian through their District-registered phone number. District employees should only contact District students for educational purposes and must never disclose confidential information possessed by the employee by virtue of his or her District employment.