California Western School of Law
E-Mail Policy
Updated July 2014

1.0 Overview

Email is an essential component of business communication; however it presents a particular set of challenges due to its potential to introduce a security threat to the network. This policy outlines expectations for appropriate, safe, and effective email use.

2.0 Purpose

The purpose of this policy is to detail the school's usage guidelines for the email system. This policy will help the school reduce risk of an email-related security incident, foster good business communications both internal and external to the school, and provide for consistent and professional application of the school's email principles.

3.0 Scope

The scope of this policy includes the school's email system in its entirety, including desktop and/or web-based email applications, server-side applications, email relays, and associated hardware. It covers all electronic mail sent from the system, as well as any external email accounts accessed from the school network.

4.0 Policy

4.1 Proper Use of School Email Systems

Users are asked to exercise common sense when sending or receiving email from school accounts. Additionally, the following applies to the proper use of the school email system.

4.1.1 Sending Email

When using a school email account, email must be addressed and sent carefully. Users should keep in mind that the school loses any control of email once it is sent external to the school network. Users must take extreme care when typing in addresses, particularly when email address auto-complete features are enabled; using the "reply all" function; or using distribution lists in order to avoid inadvertent information disclosure to an unintended recipient. Careful use of email will help the school avoid the unintentional disclosure of sensitive or non-public information.

4.1.2 Personal Use and General Guidelines

Personal usage of school email systems is discouraged. Users should use CWSL email systems for business communications only.

- The following is never permitted: spamming, harassment, communicating threats, solicitations, chain letters, or pyramid schemes. This list is not exhaustive, but is included to provide a frame of reference for types of activities

that are prohibited.

- The user is prohibited from forging email header information or attempting to impersonate another person.

- Email is an insecure method of communication, and thus information that is considered confidential or proprietary to the school may not be sent via email, regardless of the recipient, without proper encryption.

- It is school policy not to open email attachments from unknown senders, or when such attachments are unexpected.

- Email systems were not designed to transfer large files and as such emails should not contain attachments of excessive file size.

Please note that the topics above may be covered in more detail in other sections of this policy.

4.1.3 Business Communications and Email

The school uses email as an important communication medium for business operations. Users of the CWSL email system are expected to check and respond to email in a consistent and timely manner during business hours.

Additionally, users are asked to recognize that email sent from a school account reflects on the school, and, as such, email must be used with professionalism and courtesy.

4.1.4 Email Signature

Email signatures (contact information appended to the bottom of each outgoing email) may or may not be used, at the discretion of the individual user. Users must keep any email signatures professional in nature.

4.1.5 Auto-Responders

An auto-responder can be a useful tool when a user will be out of the office for an extended period of time. The school neither requires nor forbids the use of email auto-responders.

4.1.6 Mass Emailing

The school makes the distinction between the sending of mass emails and the sending of unsolicited email (spam). Mass emails may be useful (such as when communicating with the school's employees or customer base), and is allowed as the situation dictates. The sending of spam, on the other hand, is strictly prohibited.

4.1.7 Opening Attachments

Users must use care when opening email attachments. Viruses, Trojans, and other malware can be easily delivered as an email attachment. Users should:

- Never open unexpected email attachments.

- Never open email attachments from unknown sources.

- Never click links within email messages unless he or she is certain of the link's safety. It is often best to copy and paste the link into your web browser, or retype the URL, as specially-formatted emails can hide a malicious URL.

The school may use methods to block what it considers to be dangerous or strip potentially harmful email attachments as it deems necessary.

4.1.8 Monitoring and Privacy

Users should expect no privacy when using the CWSL network or school resources. Such use may include but is not limited to: transmission and storage of files, data, and messages. The school reserves the right to monitor any and all use of the computer network. To ensure compliance with school policies this may include the interception and review of any emails, or other messages sent or received, inspection of data stored on personal file directories, hard disks, and removable media.

4.1.9 School Ownership of Email

Users should be advised that the school owns and maintains all legal rights to its email systems and network, and thus any email passing through these systems is owned by the school and it may be subject to use for purposes not be anticipated by the user. Keep in mind that email may be backed up, otherwise copied, retained, or used for legal, disciplinary, or other reasons. Additionally, the user should be advised that email sent to or from certain public or governmental entities may be considered public record.

4.1.10 Contents of Received Emails

Users must understand that the school has little control over the contents of inbound email, and that this email may contain material that the user finds offensive. If unsolicited email becomes a problem, the school may attempt to reduce the amount of this email that the users receive, however no solution will be 100 percent effective. The best course of action is to not open emails that, in the user's opinion, seem suspicious. If the user is particularly concerned about an email, or believes that it contains illegal content, he or she should notify IT.

4.1.11 Access to Email from Mobile Phones

Many mobile phones or other devices, often called smartphones, provide the

capability to send and receive email. The school permits users to access the school email system from a mobile device.

4.1.12 Email Regulations

Any specific regulations (industry, governmental, legal, etc.) relating to the school's use or retention of email communications must be followed.

4.2 External and/or Personal Email Accounts

The school recognizes that users may have personal email accounts in addition to their school-provided account. The following sections apply to non-school provided email accounts:

4.2.1 Use for School Business

Users must use the CWSL email system for all business-related email. Users are prohibited from sending business email from a non-school-provided email account.

4.2.2 Access from the School Network

Users are discouraged from accessing external or personal email accounts from the CWSL network during work hours.

4.2.3 Use for Personal Reasons

Users are encouraged, but not required, to use non-school-provided (personal) email accounts for any personal communications.

4.3 Confidential Data and Email

The following sections relate to confidential data and email:

4.3.1 Passwords

As with any school passwords, passwords used to access email accounts must be kept confidential and used in adherence with the Password Policy. At the discretion of the IT Executive Director, the school may further secure email with certificates, two factor authentication, or another security mechanism.

4.3.2 Emailing Confidential Data

Email is an insecure means of communication. Users should think of email as they would a postcard, which, like email, can be intercepted and read on the way to its intended recipient.

The school requires that any email containing confidential information sent external to the school be encrypted using commercial-grade, strong encryption. Encryption is encouraged, but not required, for emails containing confidential information sent internal to the school. When in doubt, encryption should be used

4.4 School Administration of Email

The school will use its best effort to administer the school's email system in a manner that allows the user to both be productive while working as well as reduce the risk of an email-related security incident.

4.4.1 Filtering of Email

A good way to mitigate risk from email is to filter it before it reaches the user so that the user receives only safe, business-related messages. For this reason, the school will filter email at the Internet gateway and/or the mail server, in an attempt to filter out spam, viruses, or other messages that may be deemed A) contrary to this policy, or B) a potential risk to the school's IT security. No method of email filtering is 100 percent effective, so the user is asked additionally to be cognizant of this policy and use common sense when opening emails.

Additionally, many email and/or anti-malware programs will identify and quarantine emails that it deems suspicious. On occasion the filters will catch legitimate email. The users need to check their spam and junk mail regularly. Legitimate items can be “white listed” to be allowed through in the future and IT can assist.

4.4.2 Email Disclaimers

The use of an email disclaimer, usually as text appended to the end of every outgoing email message, is often recommended as an additional component of a school's risk reduction efforts. At this time the school does not require the use of email disclaimers.

4.4.3 Email Deletion

Users are required to delete email periodically when the email is no longer needed for business purposes. The goal of this policy is to keep the size of the user's email account manageable, and reduce the burden on the school to store and backup unnecessary email messages.

However, users are strictly forbidden from deleting email in an attempt to hide a violation of this or another school policy. Further, email must not be deleted when there is an active investigation or litigation where that email may be relevant.

4.4.4 Retention and Backup

Email will be backed up offsite nightly for disaster recovery purposes and is overwritten each night. We do not backup email onsite and are not able to recreate mailboxes for any point in time other than the previous night.

Unless otherwise indicated, for the purposes of backup and retention, email

should be considered operational data.

4.4.5 Address Format

Email addresses will be constructed in a standard format in order to maintain consistency across the school. The intent of this policy is to simplify email communication as well as provide a professional appearance.

4.4.6 Email Aliases

Often the use of an email alias, which is a generic address that forwards email to a user account, is a good idea when the email address needs to be in the public domain, such as on the Internet. Aliases reduce the exposure of unnecessary information, such as the address format for school email, as well as (often) the names of school employees who handle certain functions. Keeping this information private can decrease risk by reducing the chances of a social engineering attack.

Examples of commonly used email aliases are:

- admissions@cwsl.edu
- registrar@cwsl.edu

The school may or may not use email aliases, as deemed appropriate by the IT Executive Director and/or Cabinet. Aliases may be used inconsistently, meaning: the school may decide that aliases are appropriate in some situations but not others depending on the perceived level of risk.

4.4.7 Account Activation

Email accounts will be set up for each user determined to have a business need to send and receive school email. Accounts will be set up at the time a new hire starts with the school, or when a promotion or change in work responsibilities for an existing employee creates the need to send and receive email.

At times, email accounts may be given to non-employees, contractors, or other individuals authorized to conduct certain aspects of the school's business.

4.4.8 Account Termination

When a user leaves the school, or his or her email access is officially terminated for another reason, the school will disable the user's access to the account by password change, disabling the account, or another method. The school is under no obligation to block the account from receiving email, and may continue to forward inbound email sent to that account to another user, or set up an auto-response to notify the sender that the user is no longer employed by the school. Occasionally arrangements may be made to keep email.

4.4.9 Storage Limits

As part of the email service, email storage may be provided on school servers or other devices. The email account storage size must be limited to what is reasonable for each employee, at the determination of the IT Executive Director. Storage limits may vary by employee or position within the school.

4.5 Prohibited Actions

The following actions shall constitute unacceptable use of the CWSL email system. This list is not exhaustive, but is included to provide a frame of reference for types of activities that are deemed unacceptable. The user may not use the CWSL email system to:

- Send any information that is illegal under applicable laws.

- Access another user's email account without A) the knowledge or permission of that user - which should only occur in extreme circumstances, or B) the approval of the Cabinet in the case of an investigation, or C) when such access constitutes a function of the employee's normal job responsibilities.

- Send any emails that may cause embarrassment, damage to reputation, or other harm to the school.

- Disseminate defamatory, discriminatory, vilifying, sexist, racist, abusive, rude, harassing, annoying, insulting, threatening, obscene or otherwise inappropriate messages or media.

- Send emails that cause disruption to the workplace environment or create a hostile workplace. This includes sending emails that are intentionally inflammatory, or that include information not conducive to a professional working atmosphere.

- Make fraudulent offers for products or services.

- Attempt to impersonate another person or forge an email header.

- Send spam, solicitations, chain letters, or pyramid schemes.

- Knowingly misrepresent the school's capabilities, business practices, warranties, pricing, or policies.

- Conduct non-school-related business.

The school may take steps to report and prosecute violations of this policy, in accordance with school standards and applicable laws.

4.5.1 Data Leakage

Data can leave the network in a number of ways. Often this occurs unintentionally by a user with good intentions. For this reason, email poses a particular challenge to the school's control of its data.

Unauthorized emailing of school data, confidential or otherwise, to external email accounts for the purpose of saving this data external to school systems is prohibited. If a user needs access to information from external systems (such as from home or while traveling), that user must consult his or her supervisor rather than emailing the data to a personal account or otherwise removing it from school systems.

The school may employ data loss prevention techniques to protect against leakage of confidential data at the discretion of the IT Executive Director.

4.5.2 Sending Large Emails

Email systems were not designed to transfer large files and as such emails should not contain attachments of excessive file size. The school asks that the user limit the use of large email attachments.

The user is further asked to recognize the additive effect of large email attachments when sent to multiple recipients, and use restraint when sending large files to more than one person.

4.6 Applicability of Other Policies

This document is part of the school's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

5.0 Enforcement

This policy will be enforced by the IT Executive Director and/or the Cabinet. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities are suspected, the school may report such activities to the applicable authorities. If any provision of this policy is found to be unenforceable or voided for any reason, such invalidation will not affect any remaining provisions, which will remain in force.

6.0 Definitions

Auto Responder Email function that sends a predetermined response to anyone who sends an email to a certain address. Often used by employees who will not have

access to email for an extended period of time, to notify senders of their absence.

Certificate Also called a "Digital Certificate." A file that confirms the identity of an entity, such as a school or person. Often used in VPN and encryption management to establish trust of the remote entity.

Data Leakage Also called Data Loss, data leakage refers to data or intellectual property that is pilfered in small amounts or otherwise removed from the network or computer systems. Data leakage is sometimes malicious and sometimes inadvertent by users with good intentions.

Email Short for electronic mail, email refers to electronic letters and other communication sent between networked computer users, either within a school or between companies.

Encryption The process of encoding data with an algorithm so that it is unintelligible and secure without the key. Used to protect data during transmission or while stored.

Mobile Device A portable device that can be used for certain applications and data storage. Examples are PDAs or Smartphones.

Password A sequence of characters that is used to authenticate a user to a file, computer, network, or other device. This is also known as a passphrase or passcode.

Spam Unsolicited bulk email. Spam often includes advertisements, but can include malware, links to infected websites, or other malicious or objectionable content.

Smartphone A mobile telephone that offers additional applications, such as PDA functions and email.

Two Factor Authentication A means of authenticating a user that utilizes two methods: something the user has, and something the user knows. Examples are smart cards, tokens, or biometrics, in combination with a password.