Recommended

WASHINGTON CENTRAL UNIFIED UNION SCHOOL DISTRICT

Board of Directors' Policy

ELECTRONIC MAIL

POLICY: F47

WARNED: _____

ADOPTED: _____

EFFECTIVE: _____

Overview

Electronic email is pervasively used in almost all industry verticals and is often the primary communication and awareness method within the district. At the same time, misuse of email can post many legal, privacy and security risks, thus it's important for users to understand the appropriate use of electronic communications.

Purpose

The purpose of this email policy is to ensure the proper use of WCUUSD email system and make users aware of what WCUUSD deems as acceptable and unacceptable use of its email system. This policy outlines the minimum requirements for use of email within WCUUSD Network.

Scope

This policy covers appropriate use of any email sent from a WCUUSD email address and applies to all employees, vendors, and agents operating on behalf of WCUUSD.

Definitions

FERPA - The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student when he or she reaches the age of 18 or attends a school beyond the high school level. Students to whom the rights have transferred are "eligible students."

- Parents or eligible students have the right to inspect and review the student's education records maintained by the school. Schools are not required to provide copies of records unless, for reasons such as great distance, it is impossible for parents or eligible students to review the records. Schools may charge a fee for copies.
- Parents or eligible students have the right to request that a school correct records which they believe to be inaccurate or misleading. If the school decides not to amend the record, the parent or eligible student then has the right to a formal hearing. After the hearing, if the school still decides not to amend the record, the parent or eligible student has the right to place a statement with the record setting forth his or her view about the contested information.
- Generally, schools must have written permission from the parent or eligible student in order to release any information from a student's education record. However, FERPA allows schools to

disclose those records, without consent, to the following parties or under the following conditions (34 CFR § 99.31):

- School officials with legitimate educational interest;
- Other schools to which a student is transferring;
- Specified officials for audit or evaluation purposes;
- Appropriate parties in connection with financial aid to a student;
- Organizations conducting certain studies for or on behalf of the school;
- Accrediting organizations;
- To comply with a judicial order or lawfully issued subpoena;
- Appropriate officials in cases of health and safety emergencies; and
- State and local authorities, within a juvenile justice system, pursuant to specific State law.

Schools may disclose, without consent, "directory" information such as a student's name, address, telephone number, date and place of birth, honors and awards, and dates of attendance. However, schools must tell parents and eligible students about directory information and allow parents and eligible students a reasonable amount of time to request that the school not disclose directory information about them. Schools must notify parents and eligible students annually of their rights under FERPA. The actual means of notification (special letter, inclusion in a PTA bulletin, student handbook, or newspaper article) is left to the discretion of each school.

HIPAA - The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. The US Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule to implement the requirements of HIPAA. The HIPAA Security Rule protects a subset of information covered by the Privacy Rule.

PCI - The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that ALL companies that accept, process, store or transmit credit card information maintain a secure environment.

The Payment Card Industry Security Standards Council (PCI SSC) was launched on September 7, 2006 to manage the ongoing evolution of the Payment Card Industry (PCI) security standards with a focus on improving payment account security throughout the transaction process. The PCI DSS is administered and managed by the PCI SSC (www.pcisecuritystandards.org), an independent body that was created by the major payment card brands (Visa, MasterCard, American Express, Discover and JCB.).

The PCI DSS applies to ANY organization, regardless of size or number of transactions, that accepts, transmits or stores any cardholder data.

FOIA - The **Freedom of Information Act** (**FOIA**), is a federal freedom of information law that requires the full or partial disclosure of previously unreleased information and documents controlled by the public organizations. The act defines agency records subject to disclosure, outlines mandatory disclosure procedures, and defines nine exemptions to the statute. The act was intended to make U.S. government agencies' functions more transparent so that the American public could more easily

identify problems in government functioning and put pressure on Congress, agency officials, local officials and the president to address them.

Policy

- All use of email must be consistent with WCUUSD policies and procedures of ethical conduct, safety, compliance with applicable laws and proper district practices.
- WCUUSD email account should be used primarily for WCUUSD district-related purposes; personal communication is permitted on a limited basis, but non-WCUUSD related business uses are prohibited.
- All WCUUSD data contained within an email message or an attachment must be secured according to the Data Protection Standard, state and federal laws and should adhere to all FERPA, HIPAA, FOIA and PCI requirements.
- Email should be retained only if it qualifies as a WCUUSD district record. Email is a WCUUSD district record if there exists a legitimate and ongoing district reason to preserve the information contained in the email.
- Email that is identified as a WCUUSD district record shall be retained according to WCUUSD Record Retention Schedule.
- The WCUUSD email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any WCUUSD employee should report the matter to their supervisor immediately.
- Users are prohibited from automatically forwarding WCUUSD email to a third-party email system. Individual messages which are forwarded by the user must not contain WCUUSD confidential or above information.
- Users are prohibited from using third-party email systems and storage servers such as Google, Yahoo, and MSN Hotmail etc. to conduct WCUUSD business, to create or memorialize any binding transactions, or to store or retain email on behalf of WCUUSD. Such communications and transactions should be conducted through proper channels using WCUUSD-approved documentation.
- Using a reasonable amount of WCUUSD resources for personal emails is acceptable, but non-*work-related* email shall be saved in a separate folder from work related email. Sending chain letters or joke emails from a WCUUSD email account is prohibited.
- WCUUSD employees shall have no expectation of privacy in anything they store, send or receive on the district's email system.
- WCUUSD may monitor messages without prior notice. WCUUSD is not obliged to monitor email messages.

The Internet has been plagued with hoaxes alleging various security problems. Many of these hoaxes take the form of phishing attacks or chain letters, which request that the receiving party send the message to other people. Service users in receipt of information about system vulnerabilities should forward it to the WCUUSD Information Technology Helpdesk (ithelp@u32.org), who will then determine what if any action is appropriate. Service users must not personally redistribute system vulnerability information.

Distribution of Unsolicited WCUUSD Marketing: Service users must not use facsimile (fax) machines, electronic mail, instant messenger, auto-dialer robot voice systems, or any other electronic communications systems for the distribution of unsolicited advertising material.