Washington Central Unified Union School District

WCUUSD exists to nurture and inspire in all students the passion, creativity and power to contribute to their local and global communities.

1130 Gallison Hill Road
Montpelier, VT 05602
Phone (802) 229-0553
Fax (802) 229-2761

Bryan Olkowski.
Superintendent

WCUUSD Policy Committee
Meeting Agenda
12.8.20 4:30-6:30 pm

Via Video Conference*

https://tinyurl.com/y3nzqxpp
Meeting ID: 879 3885 4655
Password: 582504
Dial by Your Location 1-929-205-6099

1. Call to Order

2. Approve Minutes of 11.11.20 – pg. 2

3. Information Security Policy Review and Discussion – pg. 6

4. Policy Update
   - 4.1. E46 Memorial Policy
   - 4.2. C13 Homeless Students
   - 4.3. School Choice
   - 4.4. School Closure

5. Future Agenda Items

6. Adjourn

***Open Meeting Law temporary changes as of 3/30/20:**
Boards are not required to designate a physical meeting location. Board members and staff are not required to be present at a designated meeting location. Our building will not be open for meetings. All are welcome to attend virtually.

Washington Central Unified Union School District

WCUUSD exists to nurture and inspire in all students the passion, creativity and power to contribute to their local and global communities.

1130 Gallison Hill Road
Montpelier, VT 05602
Phone (802) 229-0553
Fax (802) 229-2761

Bryan Olkowski
Superintendent

WCUUSD Policy Committee
Meeting
November 11, 2020

Present: Superintendent Olkowski, Jody Emerson, Aaron Boynton, Michelle Ksepka, Chris McVeigh, Dorothy Naylor, Jaiel Pulskamp, Ellen Knoedler

1. **Call to Order:** Chris McVeigh called the meeting to order at 4:36 p.m.

2. **Approve Minutes of 10.27.20:** Jaiel Pulskamp moved to approve the minutes of October 27, 2020. Seconded by Dorothy Naylor, this motion carried unanimously.

3. **Review Existing Policies**

3.1 C12 Prevention of Sexual Harassment Title IX with Procedures:

Superintendent Olkowski noted that he had checked with legal counsel and that, for this particular policy, procedures should be included in the body of the policy. Jody Emerson spoke about some of the impacts of this new policy - some people might opt to not report, as there is no guarantee of confidentiality. Superintendent Olkowski indicated that he would not be surprised if this policy is revisited in the future with new administration (presidency) on board in 2021. Jaiel Pulskamp asked, what can we do as a district to alleviate that? Superintendent Olkowski indicated that this policy has been vetted by legal counsel and he thinks that we probably need to adopt this policy but expect to amend it in the future.

Jody Emerson indicated that the recommendation is that we adopt this policy with the same language that is provided. Chris McVeigh wondered whether it is required or recommended.

This policy, as is required, will go to the board for second reading/ adoption at the next board meeting.

Chris McVeigh asked - is there a mechanism to find out, when this policy is implemented, what are the difficult parts? E.g. people not moving forward with complaints because of the way the policy is written. He would like to share that question with Kelly Bushey.

4. New Required Model Policies:

4.1 C13 Homeless Students:

This policy is from the VSBA website. Chris McVeigh asked, is this a required policy according to the VSBA? Or according to some other entity? Superintendent Olkowski referred to the law (McKinney-Vento) that speaks to homelessness in schools. He asked the board to consider what is the definition of homeless; for example, students who are sleeping on couches in others' homes, on a temporary basis. Chris McVeigh stated that the definition in this policy is expansive. Dorothy Naylor asked, could we add the verbiage "including but not limited to…" under subsection (a).

Some discussion followed with Michelle Ksepka about homelessness at WCUUSD. Superintendent Olkowski spoke about the McKinney-Vento grant. He stated that a broader definition of homelessness might allow for more use of grant monies. The committee discussed some possible language for the policy:
"other situations which the superintendent and leadership team determine qualify as homelessness"
"in a situation where housing is not permanent or consistent…"
Jaiel: we could flesh out "or similar reason" more explicitly under (a)1.
Chris: change "similar" to "other" under (a)1.

Aaron Boynton stated that he worries about leaving it *too* open for interpretation. Some discussion followed around anecdotes from the past related to homelessness. Superintendent Olkowski would like to have Jen Miller Arsenault take part in this conversation. Michelle Ksepka explained the online student registration system for WCUUSD.

Superintendent Olkowski would like to have Jen Miller Arsenault take a look at this policy before we move forward with it. The committee agreed to put this on the agenda for the next Policy meeting, and to invite Jen Miller Arsenault.

4.2 B8 Electronic Communication between Employees and Students:

Superintendent Olkowski indicated that he believes we need this policy in a timely manner; he would like to get some input from Jim Garrity as well.

Chris McVeigh asked the administrators what they believe is needed to be included in these policies.

Superintendent Olkowski indicated that it is important to identify what is "inappropriate communication." Chris McVeigh asked whether we should be asking for parental consent. Jody Emerson stated that she believes there is already parent consent included in the electronic use agreement.

Some discussion followed around times of day (e.g., late at night) that these communications are appropriate, or not. Aaron Boynton indicated that he thinks restricting hours or creating curfews does not address the core issue.

Jody Emerson asked about the definitions under "inappropriate content of electronic communication" not allowing for communications related to social or emotional well-being.

Discussion followed around this topic. Ellen Knoedler asked if there is currently a policy that indicates that teachers can't or shouldn't be friends with students on Facebook or Twitter, or anything like that?

Chris McVeigh suggested, should we consider "no electronic relationships with students" (except email)?

Dorothy Naylor asked whether substitutes are included in this policy.

Superintendent Olkowski asked whether we are trying to include too much in this policy? Some districts have a separate social media policy.

Some discussion followed around email communication being considered part of permanent educational record.

Superintendent Olkowski suggested continuing this conversation with Jim Garrity present.

Chris McVeigh asked whether the committee would like to consider a separate social media policy. Or, he suggested the possibility of adding to this policy "teachers should not have social media friendships with students under the age of 18." He would like to see if this is a violation of First Amendment rights.

The committee will address this at the next Policy Committee meeting.

Superintendent Olkowski stated that it might be helpful for Jim Garrity to consider some changes in the language to this policy that the committee is considering.

Chris McVeigh stated that if we were going to change the policy to include social media we would need to change the *statement of policy* section to include social media. Jody Emerson stated that there are several social media groups that are affiliated with school groups or clubs.

Jaiel Pulskamp stated that she would like to see some sample policies from other schools. Chris McVeigh will reach out to the Agency of Education to see if they are aware of other districts that have social media policies.

5. Policy Creation

5.1 School Choice

5.2 School Closure

Brief conversation followed around COVID19 updates and upcoming holidays and travel.

Aaron Boynton explained that grades K-8 are putting off winter sports until after the new year when they will reconsider, depending on the status of COVID19.

Dorothy Naylor stated that she does not think it is wise for the board or administration to do anything that encourages travel.

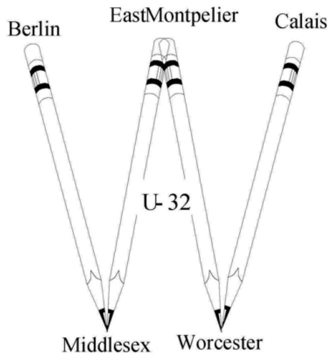
6. Future Agenda Items:

- Memorial Policy - with principals' feedback (also sample letters to notify families)
- Next meeting date: Tuesday, December 1, 2020.
  4:30 - 6:30 (will invite Jen Miller Arsenault and Jim Garrity)

7. Adjourn: The committee adjourned at 6:28 p.m.

Respectfully submitted,
Lisa Stoudt, Committee Recording Secretary

Washington Central Unified Union School District



Information Security Policy

Revision History

Date	Changed By	Revision #	Comments
11/25/2020	Jim Garrity	v.0.5	Draft Information Security Policy Released

Policy Committee Approval History

Date	Approved By	Comments

POLICY

Defining the Overall Approach toward Meeting a Requirement

Table of Contents

1 Introduction

Washington Central Unified Union School District (WCUUSD) Information Security Policy defines the technical controls and security configurations uses and implemented in order to ensure the confidentiality, integrity and availability of the data and systems used at WCUUSD. It serves as a central policy document with which all employees must be familiar and defines actions and prohibitions that all users must follow. The policy provides WCUUSD staff with policies and guidelines concerning the acceptable use of WCUUSD'S technology equipment e-mail, Internet connections, voicemail, facsimile, technology resources, and information processing.

The security policy is one key element of the broader security framework and represents a single facet of the overall control framework implementation within the organization. The information security policy works in tandem with documented standards, procedures, and other policies to provide WCUUSD with a solid foundation upon which to carry out the information security program and protect critical business functions.

In order to protect important business assets and facilitate proper mission critical functions, WCUUSD'S information must be properly protected from disclosure, alteration, or destruction whether intentional or accidental. Since a loss or compromise of critical information systems could negatively impact WCUUSD, its workforce including staff, students, volunteers, contractors, etc. must read, understand, and follow this policy or be subject to the appropriate corrective actions. Further, access to this Information Security Policy will be available to all employees, and training will be provided to ensure that individuals are able to properly review and understand the policy's requirements.

The key principals of the Information Security Policy include:

- Protection of WCUUSD'S information systems, applications, student information, products, and data against a loss of confidentiality, integrity, or availability.
- Periodic assessment of system risk to identify and mitigate security vulnerabilities.
- Implement supplemental processes, procedures, and standards that support the WCUUSD security program and initiatives.
- Ensure that appropriate controls are implemented to protect data and resources, including: encryption standards, approved security tools, and business partner agreements.
- Protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer.

- Provide an understanding of WCUUSD'S regulatory compliance and industry security standards (e.g., NIST, FERPA, ISO, and HIPAA) requirements.
- Enforce approved policies and procedures by following documented sanction policies for violations.

The policy requirements and restrictions defined herein shall apply to network infrastructures, databases, external media, encryption, hardcopy reports, wireless, telecommunication, conversations, and any other methods used to convey knowledge and ideas across all hardware, software, and data transmission mechanisms

2 Purpose

The purpose of this document is to provide guiding policy for protection of the sensitive data environment for students, teachers, and administrators to the full extent of the standards established by law. WCUUSD has and will continue to establish, publish, maintain, and disseminate security policies in response to changes in the organizations environment, periodically in accordance with current and subsequent updates to the regulatory requirements. Additionally, WCUUSD will consult with their legal consul at least annually to ensure adherence with any applicable laws and regulations.

3 Scope

This policy defines common security requirements for all WCUUSD personnel and systems that create, maintain, store, access, process or transmit information.

This policy also applies to information resources owned by others, such as vendors and contractors of WCUUSD such as the entities in the private sector, in cases where WCUUSD has a legal, contractual or fiduciary duty to protect said resources while in WCUUSD'S custody. In the event of a conflict, the more restrictive measures apply.

This policy covers WCUUSD'S network system, which is comprised of various hardware, software, communication equipment, and other devices designed to assist the organization in the creation, receipt, storage, processing, and transmission of information. This definition includes equipment connected to any WCUUSD domain, either hardwired or wirelessly, and includes all stand-alone equipment that is deployed by WCUUSD at its office locations or at remote locales.

4 Information Security Policy Owner

The Director of Technology (DTO) with assistance by the Information Security Officer (ISO) (“WCUUSD Policy Committee” herein) shall be the owner of this document and any other Information Security and/or Information Technology Policy Series. As the owner of these documents, the WCUUSD Policy Committee shall be responsible for maintaining and ensuring the review of this policy by department managers or as defined in the policy and procedures review process.

WCUUSD policies and procedures are submitted to the WCUUSD Policy Committee for review and approval. Once approved by the DTO, the policy and/or procedure is placed in WCUUSD’S Google Drive for access by the appropriate departments/individuals.

Updates to the policy may occur in response to any changes that would affect the assumptions from the baseline risk assessment, such as significant security incidents, new vulnerabilities, new regulations or changes to the organization’s infrastructure. This and all Information Security and/or Information Technology policies and procedures will be reviewed periodically and those containing major revisions will be submitted to the DTO for review and approval.

WCUUSD shall not be liable for any damages of any nature suffered by any customer, user, and/or any third party resulting in whole or in part from WCUUSD’S exercise of its rights under these policies.

5 Support Regarding Information Security

Service Continuity / Information Technology Internal Support: The primary method for gaining support on internal computing systems will be by sending e-mail using the WCUUSD Information Technology Helpdesk (ithelp@u32.org). WCUUSD users should use this as the point of contact for all desktop, workstation, servers, storage, and email support issues.

Security Operations: For situations regarding electronic mail abuse, direct violations of security policy, attempted intrusions, or possible breaches of internal security please contact the WCUUSD Information Technology Helpdesk ithelp@u32.org, who will coordinate with the WCUUSD IT Director or Security Team. In times of emergencyplease follow the documented internal escalation procedures. Investigations of system intrusions and other information security incidents surrounding customers should be handled through the use of the outlined steps created by the WCUUSD IT Team (including KB articles and other documented security handling procedures).

6 Enforcement

The WCUUSD Policy Committee or designee will randomly evaluate the requirements outlined in each of the policies in this series. If the evaluation uncovers a violation of this policy, it must be communicated to the appropriate manager immediately.

Any user which WCUUSD determines, in its sole discretion, to have violated any element of this Information Security Policy and/or Information Technology related policies and procedures shall be subject to disciplinary action up to and including termination of employment. Non-compliance or violation of this policy, by any WCUUSD User will result in actions that may include but are not limited to the following:

- Warning (verbal or written)
- Suspension
- Termination

Additionally, non-compliance or violation of this policy by a temporary worker, contractor, or vendor may result in the termination of their contract or assignment with WCUUSD.

All Users of WCUUSD'S system resources are responsible for promptly reporting any violation of this policy or potential violations and should immediately notify their manager and/or the WCUUSD Policy Committee.

It is everyone's responsibility to report a suspected or actual breach of security.

7 Roles and Responsibilities

The following list summarizes the key roles for WCUUSD. These roles are explicitly listed in order to provide structure to the overall security program. The department managers shown below are responsible for all aspects of ensuring security and compliance as well as developing, implementing and annually reviewing and/or updating their Standard Operating Procedures (SOPs) for their departments

- **Availability-** is designated as WCUUSD'S systems owner and is responsible for the oversight of internal and customer supporting systems.
- **Human Resources** – is designated as having responsibility for WCUUSD'S various aspects of employment, such as compliance with labor law and employment standards, administration of employee benefits, and some aspects of recruitment and dismissal process.
- **Service Continuity / IT -** is designed by WCUUSD as having responsibility for IT requirements for WCUUSD staff.
- **Security Operations**– is designated by the WCUUSD ISO as having day to day responsibility for managing and creating the security program.
- **Users** – are employees, volunteers, contractors, or other individuals that have been explicitly given access to WCUUSD'S resources and/or data. Authorized users will be responsible for utilizing the information they have access to only for authorized business purposes. Further, they will maintain the integrity, confidentiality, and availability of all accessed information.

All policies, procedures, knowledge-based documentation, etc. will be placed in the SharePoint to ensure the information is available to WCUUSD employees and contractors.

8 General Use and Governance

The security initiative at WCUUSD is driven by IT who develops policy and coordinates its enforcement with the teachers, students, the board, outside vendors, the ISO, development leaders and the executive team. The areas of security addressed by these individuals are:

Physical Security - It includes monitoring and administration of building access, the alarm systems and video surveillance systems.

Network & Workstation Security - This area of security is the responsibility of the IT organization under the leadership of the Director of Technology. IT manages the configuration of network and systems devices and communications. They will report system and security concerns, configuration requests and issues to the Director of Technology and IT teams.

Application Security - This area of security is the responsibility of the Director of Technology who oversees the testing and implementation of internal applications used to operate the business and provide customer support.

System Security - This area of security is the responsibility of our IT Department. This group is responsible for the building and administration of internal and customer systems, performs backup and recovery services, patch management and virus protection.

The **WCUUSD Policy Committee** is also responsible for the development, implementation, enforcement and education of security policies covering all four of the defined security areas.

9 Information Security Policy Details

9.0 Network Management Policy

9.0.1 Purpose

The WCUUSD computing network is critical to the provision of information services to the organizations staff and clients. The WCUUSD system processes sensitive and valuable information. The need to secure sensitive data has increased the size, complexity, and management concerns related to the operation of the network. Specific security measures and procedures must be implemented to protect the confidentiality of information transactions being processed on the network and to keep critical systems operational. Because of the connection to outside services including the internet, security risks have increased and more stringent practice in safeguarding resources is necessary than was required when simple standalone PCs were used. These expanding security requirements are addressed in the following security policy.

This policy has two purposes. First, the policy will emphasize to all WCUUSD employees the importance of network security and their roles in maintaining that security. Second, the policy will assign specific responsibilities needed to secure networked information resources.

9.0.2 Scope

WCUUSD'S Information Security Policy covers all electronic information resources in the organization. It applies equally to network servers, workstations, network equipment, telecommunications equipment, and peripherals, such as printers, within the corporation.

This policy applies to all personnel, managers, administrators, and contractors utilizing WCUUSD'S network resources.

9.0.3 Goals

The security program is designed to ensure the availability of networked resources and introduce controls designed to bolster the integrity and confidentiality of data transmitted over and stored on the network. Specifically, the goals of the program include:

- Ensuring the network has sufficient security measures applied to protect the sensitive data, the privacy of information transactions, and the availability of its resources.
- Ensuring the cost of the security measures implemented is commensurate with the risks present on the network.
- Ensuring appropriate budgetary and technical support is available and maintained.
- Training all users to be responsible for the security of data, information, and other computing resources to which they have access, and training staff to maintain accountability practices.
- Enforcing policies and technical mechanisms which contribute to the audit ability of network resources.

- Providing sufficient guidance to staff in the discharge of their responsibilities in network and information security.
- Ensuring that all applicable organizational and departmental policies and procedures are applied and practiced.
- Developing appropriate contingency or disaster recovery plans to provide continuity of operation for all critical functions of the network.

9.0.4 Specific Responsibilities

9.0.4.1 End Users (EU)

Users are expected to be knowledgeable about and adhere to WCUUSD'S Acceptable Use Policies and are ultimately responsible for their own behavior. User responsibilities include but are not limited to the following:

- Understanding and respecting relevant Federal and State laws, FERPA, HIPAA, and WCUUSD policies and procedures, and other applicable security procedures and practices established for the WCUUSD network.
- Using network, system, and application resources in accordance with terms specified in WCUUSD'S Acceptable Use Policy and being aware of activities disallowed and the consequences of engaging in such unauthorized use.
- Being aware of privacy issues related to their use of network resources and protecting the confidentiality and integrity of their own information.
- Selecting and maintaining strong passwords as outlined in WCUUSD'S Password Policy. Specifically, users must not disclose unique user IDs or passwords to others.
- Notifying a local administrator when security procedures are not followed—for example, when a previous user leaves a workstation without logging off or when passwords are written and left in open view.
- Remote users accessing WCUUSD systems with their personal computers shall read and acknowledge their understanding of the WCUUSD Acceptable Use Policy and complete their annual Security Training.
- Notifying the WCUUSD Policy Committee if a security violation or breach is suspected, observed or detected.
- Being familiar with how malicious or virus-infected software is distributed and observing practice that minimizes the risk of damage due to the introduction of such software.
- Reporting any signs of abnormal or suspicious activity to the IT Administrators

- WCUUSD staff will ensure that his/her workstation is left on as scheduled so the hard drive may be backed up, according to the WCUUSD backup policy.

9.0.4.2 WCUUSD Administration

WCUUSD Administration is ultimately responsible for ensuring that the objectives of the Information Security Policy and individual responsibilities are clearly communicated to staff and end users and are adequately followed. Specific responsibilities of managers include:

- Effectively analyzing potential security risks in order to formulate safeguards and update or develop appropriate security policy on an annual basis. This risk management requires:
  - identifying the assets to be protected
  - assessing potential vulnerabilities
  - analyzing the risk of exploitation
  - implementing cost-effective safeguards
- Provide training to all staff in the appropriate use of the network, systems, and applications; awareness of the possible effects of misuse or unauthorized use of network resources, and the consequences of any unauthorized use. Training should occur upon hire and on an annual basis.
- Ensuring staff understand the danger of malicious software, how it is generally spread, and the technical controls used protect against it.
- Informing Human Resources, IT staff, etc. of the change in status of employees, or contract workers who utilize WCUUSD resources. This could include a position change (providing greater or more restricted access privileges) or termination of employment.
- Ensuring that new employees that have access to sensitive data are required to undergo (and pass) a background investigation as deemed required by HR or WCUUSD Administration.
- Ensuring IT Administrators and management govern access to any system or element in the sensitive data environment in accordance with the following parameters:
  - User access rights are reviewed on an annual basis and access rights are based on job classification and function (role-based access control), restricted to the least privileges necessary to perform job responsibilities, and access control systems are configured using a default deny all setting
  - Authorization forms signed are used to grant access, and access controls are implemented via automated systems

9.0.4.3 IT Department / Service Continuity

IT Department / Service Continuity may include local staff or contracted support. The IT Department / Service Continuity is expected to implement and maintain security measures to enforce security policies, archive critical programs and sensitive data and control logical and physical access to network facilities. Specifically, network management is responsible for:

- Rigorously applying available security measures enforcing local security policies.
- Advising IT on the effectiveness of the existing policies and technical considerations that may lead to improved practices.
- Responsible for securing the local network and its borders with outside network.
- Responsible for notifying IT of and responding to computer security incidents, security breaches or violations in a timely and effective manner.
- Cooperate with local administrators in tracking/monitoring violators and assist in enforcement efforts.
- Configuring audit logs and using network monitoring tools to aid in the monitoring, detection and investigation of security violations.
- Conducting timely audits of network logs.
- Remaining informed on outside policies and recommended security best practices and, when appropriate, informing IT of new developments.
- Exercising the powers and privileges inherent in network administration with caution and discretion.
- Monitoring and controlling all access to data.
- Administering user accounts, including additions, deletions, and modifications.
- Identifying, recommending, installing, testing, and configuring software or systems providing:
  - Intrusion detection, including network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems designed to monitor all network traffic and alert personnel to suspected compromise. Ensure detection systems are updated regularly and maintained in accordance with manufacturer's recommendations.
  - File integrity, monitoring software designed to alert personnel to unauthorized modification of critical system or content files. Configure file integrity systems to perform critical file comparisons at least weekly
  - Log management used to monitor unauthorized activities.
  - Anti-virus systems used to remove malicious software.

- Developing incident response procedures that allow for reporting security violations and notify the administration and outside agencies (when required) of any threats.
- Developing daily operational security procedures that are consistent with requirements in this specification (e.g., user account maintenance procedures, and log review procedures).
- Providing assistance in tracking the source of malicious software or computer viruses and determining the extent of contamination.
- Removing malicious software or viruses.
- Establishing a process to identify newly discovered security vulnerabilities (for example, subscribe to alert services freely available on the Internet) and update configuration standards to address new vulnerability issues.
- Conducting periodic audits to ensure proper security practices are followed.
- Maintaining user privacy.

The IT / shall specifically follow the following guidelines:

- Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.
- Implement automated audit trails for all system components to reconstruct the following events:
  - All individual accesses to sensitive data
  - All actions taken by any individual with root or administrative privileges
  - Access to all audit trails
  - Invalid logical access attempts
  - Use of identification and authentication mechanisms
  - Initialization of the audit logs
  - Creation and deletion of system-level objects

- Record at least the following audit trail entries for all system components for each event:
  - User identification
  - Type of event
  - Date and time
  - Success or failure indication
  - Origination of event
  - Identity or name of affected data, system component, or resource
  - Synchronize all critical system clocks and times
- Synchronize all critical system clocks and times
- Secure audit trails so they cannot be altered

  - Limit viewing of audit trails to those with a job-related need
  - Protect audit trail files from unauthorized modifications
  - Promptly back up audit trail files to a centralized log server or media that is difficult to alter.
  - Copy logs for wireless networks onto a log server on the internal LAN
  - Use file integrity monitoring and change detection software on logs to ensure that existing log data cannot be changed without generating alerts (new data being added should not cause an alert)
- Review logs for all system components at least daily.
- Managing all users' access privileges to programs and data.
- Monitoring security-related events and following up on any actual or suspected violations, where appropriate; notifying network management of reported security incidents and assisting in investigations.
- Maintaining and protecting server software, relevant files, and media using specified security mechanisms and procedures.
- Overseeing the update of anti-virus signatures on all local workstations and servers and ensuring that hard drives are scanned regularly.
- Assigning a unique USERID and initial password to new users according to established procedures.
- Backing up all data on network servers and workstations according to established procedure.

9.0.5 Internal Network Connections

All WCUUSD computers that are permanently or intermittently connected to internal computer networks must have a password-based access control system approved by the Information Technology Department. Regardless of the network connections, all stand-alone computers handling Company information must also employ an approved password-based access control system.

Access Control Policy

Overview

All WCUUSD access is controlled by the use of keys at offices or proximity badge within parts of the building. The proximity badge is managed by IT. Access levels are defined by job requirements and management.

Purpose

This policy is designed to protect WCUUSD from unauthorized access to facility and assets.

Physical Security

For the purpose of this policy, physical security has been divided into two elements; site physical security and information asset physical security.

- **Individual Access**- Physical access to information assets is granted on a need-to-know basis to provide the minimum access to sensitive data necessary.

- **Responsibilities-** IT will be responsible for:
  - Developing, implementing, maintaining and enforcing information asset physical security policies.
  - Ensuring physical security policies and procedures are tested and reviewed at least annually.
    - Results of testing and review shall be used to make changes to policies and procedures as needed.
  - Documenting exceptions to policies and procedures and identifying compensating controls where exceptions are made.
  - Tracking all facility modifications

Identification Badges - Each employee of the facility will be issued a Photo ID and access card (or key) during their new hire orientation and office employees will be given a key to the office. All employees are expected to wear the Photo ID card at all times when on site at any facility where WCUUSD assets are stored digitally. These cards are the responsibility of each employee to maintain and keep secure. If either card is lost or stolen, the employee must notify their manager and the IT Manager of their facility immediately. The lost card will be deactivated and a new card issued.

Change Management

Overview

The objective of change management in this context is to ensure that standardized methods and procedures are used for efficient and prompt handling of all changes to control IT infrastructure, in order to minimize the number and impact of any related incidents upon service.

Purpose

To control all changes to equipment, software or procedures will be established and followed for change, integrating operational and application change control procedures, and logging all changes.

Change Management Requirements

There shall be a formal approval for proposed changes that could potentially impact the operational environment. Prior to any operational change there shall be a risk assessment that:

- Identifies significant changes.
- Records significant changes.
- Assesses the potential impact of such changes.
- Procedures and responsibilities for aborting and recovering from unsuccessful changes
- All changes shall be reviewed in advance and requires the written approval of the or designee.
- All changes shall be communicated to all relevant individuals.

Change Policies

Computers/Workstations

There shall be a formal approval for proposed Local Administrator Access: WCUUSD service users will not have the right to change the local administrator passwords on WCUUSD provided desktop computers. Service Users may request access to the local administrators group from the Information Technology Department, however, this will void the computer and the service user from being supported by the Information Technology Group. Systems that have been modified and require the assistance of the Information Technology Department will be re-loaded with the original software configuration that the Information Technology Department supplies to service users when issued a new system.

Network Configuration Changes: The standard configuration on WCUUSD laptops is configured so that in most cases the computer can be transferred from network to network without any configuration changes. If a user requires special circumstances to be accounted for, they should reference the sections: “Change policies, as related to desktop computers/workstations: Local Administrator Access” and “Remote Access Computing Policies” in this document.

Changes to Hardware: Computer equipment supplied by WCUUSD must not be altered or added to in any way (e.g., upgraded processor, expanded memory, or extra circuit boards) without prior knowledge and authorization from the Information Technology Department.

Changes NOT Related: Any changes that are not related to the changes listed above must adhere to and comply with the Corporate Change Management Policy and Procedure.

Reasonable Care in Protecting Proprietary and/or Confidential Information

When WCUUSD service users are engaged in communication involving proprietary or confidential information from external or un-trusted networks, the use of encryption must be employed. The Information Technology Department has made available policies and procedures for service users that require remote access, these systems must be used for the transmission of sensitive information. For example, the use of the corporate VPN (IPsec), Secure Sockets Layer (SSL/https) or Transport Layer Security (TLS/https) is required for accessing WCUUSD systems when dealing with sensitive information across the Internet. Resources that are not encrypted by default should be avoided.

Data Retention and Storage Policy

Overview

All WCUUSD information must be backed up to WCUUSD Network Storage or authorized Information Technology Department methods only. The use of external drives (thumb drives, UBS drives, etc.) must be approved by the IT Team.

Purpose

To ensure Data Retention and Storage of data is controlled as outlined by industry, federal and/or state requirements. Additionally, information must be consistently protected throughout its life cycle, from its origination to its destruction.

Minimize Storage and Retention of Sensitive Data

Sensitive data storage will be kept to the minimum necessary to conduct business operations. Sensitive data shall only be retained for that amount of time which is required for business, legal, and/or regulatory purposes.

At no time shall any sensitive data be stored in any form outside of approved systems without expressed written permission from authorized personnel within WCUUSD. The following storage mechanisms for sensitive information are prohibited:

- Hardcopy, including guest books, paper notes, notebooks, receipts, or any other hardcopy format.

- Personal computers, including laptops, personal digital assistants, tablets, cell phones or other PC's, whether personally owned or WCUUSD resources.

Backups

Individual User Responsibility: WCUUSD service users must ensure that information that represents any part of a business plan, system design, or that relates to the management of customer accounts are adequately protected from loss. Company file servers are frequently archived; this is the suggested method for ensuring that information loss is prevented. If a user is unable to ensure adequate loss protection, they should contact the WCUUSD Information Technology Helpdesk (ithelp@u32.org) for assistance in resolution of this problem.

Not Responsible for Backups of Personal Data: WCUUSD information systems are for official company use. WCUUSD will not backup user's personal data files or programs that are not WCUUSD property or have no relevance to WCUUSD business. Examples include but are not limited to encoded music files, digital images and games. The Information Technology Department may remove such items from WCUUSD systems at their discretion without prior warning to individuals.

General Storage Rules

- Maintain records in an appropriate storage form (i.e. paper, magnetic tape, microfilm, flash drive, optical disk) for the recommended length of time indicated by this policy.

- All records being prepared for storage should be described and include the following information on a label in order to facilitate their reference, review, and destruction:
  - The inclusive dates
  - Originating department name
  - Type of media
  - Date of destruction
  - Contact name and telephone number.

- Ensure the appropriate forms of records are complete and copies of such records can be reproduced in a complete and readable form upon request.

- Store all records in a manner that permits the efficient retrieval of stored records and the efficient return of records borrowed from storage.
- Restrict access to stored records to those individuals who have anappropriate need and permission to retrieve the records.
- Ensure all records are stored in a climate-controlled location with protection from hazards (i.e., theft, water, fire).
- Confirm that records copied onto an alternative storage medium (microfiche, diskette, tape) are complete and readable before the original paper record is destroyed. All records stored in an alternate format must be available for reading and/or duplicating within a reasonable timeframe. Once records have been transferred, the original version can be destroyed according to thispolicy.
- Protect computerized data with password, code or cardsystem.
- The Uniform Preservation of Business Records Act requires retention ofgeneral business records for three years from the creation of such records if no retention period is specified by regulation.
- Credit card transaction data should be stored only as long as required for financial tracking and auditing purposes. The specific credit card holder information such as the account number, expiration date, or other magnetic stripe information should never be stored in electronic format unless specific approval is received from the IT Department and the WCUUSD Policy Committee.

District Take Home Device & Personal Device Policy

Overview

The mission of the District Take Home Device & Personal Device Policy in WCUUSD is to create a collaborative learning environment for all learners. This environment will support students and teachers in the use of technology to enhance student learning and engagement in the classroom. It will create equity and level the playing field for all learners by providing every student with a device to use both in school and at home.

In 2019 the District expanded the use of Chromebooks and the ability for students to take home the devices to support their schoolwork. Students at all WCUUSD schools will have the opportunity to check out a district-owned Chromebook (Grades 3-12) or Tablets (Grades PreK-2) for the school year. This device will allow filtered access via the district network to educational resources and materials needed for students to be successful. It will also allow all student access to G Suite for Education, online textbooks, educational web-based tools, and many other useful websites.

Education and Access

G Suite for Education is a closed system whereby only students and staff have access. It includes applications that enable students to:

- Create projects
- Collaborate with their classmates
- Send emails to students and teachers
- Submit assignments

As a G Suite for Education District, we are able to monitor student Chromebook activity through web-based management tools.

Before each Chromebook device connects to the Internet, it must pass through district network firewalls and filters. This happens whether the device is browsing at school or home using another WiFi router that is providing the Internet connection. We are currently using Content Keeper for Chromebook and other background tools.

Daily Care and Maintenance

Students are responsible for the general care of the Chromebook they have been issued by the school. Chromebooks that are broken, or fail to work properly, must be submitted to IT or designated staff. Do not take District owned Chromebooks to an outside computer service for any type of repairs or maintenance. Do not attempt to repair the device yourself. We understand accidents happen. Report them immediately so that the district can fix the device.

- Students are responsible for bringing fully charged Chromebooks for use each school day.
- Chromebooks must have a District asset tag on them at all times and this tag must not be removed or altered in any way. If removed there may be disciplinary action.
- No food or drink is allowed next to your Chromebook while it is in use.
- Cords, cables, and removable storage devices must be inserted carefully into the Chromebook. Plug-in connectors are **fragile** and must be handled with care.
- Never transport your Chromebook with the power cord plugged in. Never store your Chromebook in your carry case or backpack while plugged in.
- Clean the screen with a soft, dry microfiber cloth or anti-static cloth. No liquids.
- Student should never leave a Chromebook unattended, such as in a vehicle or any unsupervised area.
- Transport Chromebooks with care, Chromebook lids should always be closed and tightly secured when moving.

- Never move a Chromebook by lifting from the screen. Always support a Chromebook from its base with the lid closed and open or close it using two hands.

Chromebook screens can be easily damaged! The screens are particularly sensitive to damage from excessive pressure on the screen.

- Do not store the Chromebook with the screen in the open position or tablet mode.
- Do not place anything on the Chromebook that could put pressure on the top or screen.
- Do not poke the screen with anything that will mark or scratch the screen surface.
- Do not place anything on the keyboard before closing the lid (e.g., pens or pencils)
- Do not place the device near magnets or anything with high electric current.
- Do not place anything in the sleeve or backpack that will press against the cover.

Digital Citizenship and Internet Safety

WCCUSD asks that all computing equipment is used for educational purposes or to support those employees who provide educational services. We expect device holders to use electronic resources safely and responsibly. We ask that students engage a trusted adult if you are unsure about something related to the use of your computer or electronic resources. We expect that you will not share your account information or the account information of others. Never post or share pictures of yourself or others unless you have school permission. Please tell a trusted adult if you come across something that is dangerous or disturbing. All school rules for how you behave and how you treat others apply for in-person and for electronic communications.

Security, Filtering, and Monitoring

The school district is required by law to provide certain levels of filtering and monitoring of the use of all district owned technology and electronic resources. All students are expected to support these efforts to provide a safe and legal electronic learning environment. It is expected that parents/guardians will monitor the student's use of the Internet at home so that the district-owned device is not used to access illegal or inappropriate websites or download any material from those sites. Please be aware of these cautions.

- Do not use district equipment or electronic resources for commercial or personal gain.
- Do not use district resources for political purposes, like trying to influence elections.
- Do not use district resources for anything illegal or indecent such as bullying, posting inappropriate images or text, or passing along information that is harmful or inappropriate.
- Do not participate in any activity to alter, bypass or attempt to bypass the school district network, security settings, filters, safety settings, or user roles.
- Do not install or download personal software or applications (apps), games, or operating systems.

Lost or Damaged Equipment

Students and parents will be responsible for district-owned technology that is issued to them, just as they are for other district-owned items such as textbooks, athletic equipment, or library books. The district will repair or replace the device, but students and parents may be responsible for the cost of those repairs or replaced devices. Please remind your student to report a missing Chromebook to the library staff or classroom teacher (in-person or via email) as **soon** as it's misplaced. We can help them locate. After 24 hours we will disable the device.

The WCUUSD Transportation Staff have been asked to return any found devices to the U-32 Technology Office.

Submit Chromebooks that need repair, with the sleeve and power cord to the Building Technology Specialist, teacher-librarian, or classroom teacher depending on your school. If we are able to fix the device, we will do so and return it. If we are unable to fix the problem, we will issue a new device. Physical damage or lost equipment may cost a student or employee the replacement fee of $400.

Use of Personal Electronic Devices

In accordance with all district policies and procedures, students and staff may use personal electronic devices such as, but not limited to, laptops, mobile devices, cell phones, and e-readers to promote student learning and to further the educational and research mission of the district. The use of personally owned devices at school by staff and students is voluntary and a privilege, and subject to all school district policies and procedures. School staff will retain the final authority in deciding when and how students may use personal electronic devices on school grounds and during any school-related activity.

The district assumes no liability or responsibility for any act of a staff, student or guest user that is inconsistent with school district policies and procedures. Any individual who brings personally owned devices onto school property is solely responsible for that equipment.

If the District has reasonable cause to believe a staff member or student has violated school district policies or procedures authorized personnel may confiscate and search a staff, student's or guest user's mobile device in accordance with school district policies and procedures for privacy, and search and seizure.

Password Management Policy

Overview

Strong and consistent management of user IDs and passwords enables the WCUUSD to authenticate individual users, trace actions to users, and fully utilize the secure features of the network and system infrastructure of the organization and to protect sensitive information to the fullest extent practical. All employees and personnel that manage or have access to systems and networks must adhere to the password policies defined below in order to protect the security of sensitive information and data.

Purpose

This policy applies to any and all personnel who have any form of user or administrator account requiring a password on any network, system, or system component.

Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any WCUUSD facility, has access to the WCUUSD network, or stores any non-public WCUUSD information.

User ID & Password

User-IDs and Passwords: WCUUSD requires that each service user accessing multi-user information systems have a unique user-ID and a private password. The unique user-ID and in some cases, the initial password will be issued by WCUUSD Information Technology Department. All issued passwords must be changed at first login and is enforced through group policy. These user-IDs must then be employed to restrict system privileges based on job duties, project responsibilities, and other business activities. Each service user is personally responsible for the usage of his or her user-ID and password. All activity logged under a user account is the responsibility of the user who owns the account.

Role Accounts/Anonymous User-IDs: With the exception of electronic bulletin boards, Internet web sites, and other systems where all regular users are intended to be anonymous, users are prohibited from logging into any WCUUSD system or network anonymously. Anonymous access might, for example, involve use of "guest" user-IDs. When users employ system commands that allow them to change active user-IDs to gain certain privileges, they must have initially logged-in employing user-IDs that clearly indicated their identities. This might, for example, take place on UNIX systems with the SU command. Demonstration software and/or demonstration systems for customers are exempt in that a customer may access the system anonymously; however, all administrative tasks performed by WCUUSD employees, representatives, contractors, or otherwise must not be anonymous.

Difficult-to-Guess Passwords: To ensure that password systems do the job they were intended to do, users must choose passwords that are difficult-to-guess. This means that passwords must NOT be related to one's job or personal life. For example, a car license plate number, a spouse's name, or fragments of an address must not be used. This also means passwords must not be a word found in the dictionary or some other part of speech. For example, proper names, places, technical terms, and slang must not be used. The password “WCUUSD” must never be used (regardless of upper or lower case) on network (public or private) connected systems, even for demonstration accounts or public access. The password length must be a minimum of eight alphanumeric characters with the maximum number of characters being system dependent. Creating passwords that are at least 15 characters or more can ensure a more secure environment. If words are used in your password, ensure that you are using non-compound words.

Random Characters Must be Used: At least one special character and one numeric character should be used to increase the difficulty in guessing passwords. An example would be the numeric character ‘3’ in place of the letter ‘E’. Special and Numeric characters include numbers, punctuation marks, and delimiting characters such as the “@” symbol.

Passwords Change Frequency: Passwords should only be changed when there is a reason to believe that a password has been compromised. Changes should occur every year for privileged accounts. This must be enforced by software controls on multi-user systems and within the Active Directory domain. Additionally, passwords must not be re-used. All multi-user systems, which have the capability to prevent the re-use of passwords, will not allow a user to enter a password that has been recently used, within 5 uses. Additionally, software controls may be employed that prevent the repeated changing of passwords to facilitate the minimum number of changes within a short period of time.

Password Storage: Passwords must not be stored in readable form in batch files, automatic log-in scripts, software macros, terminal function keys, in computers without access control systems, or in other locations where unauthorized persons might discover them. Similarly, passwords must not be written down in some readily decipherable form and left in a place where unauthorized persons might discover them.

Sharing Passwords: If users need to share computer-resident data, they should use electronic mail, group-ware databases, public directories on local area network servers, and other similar mechanisms. Although user-IDs are shared for electronic mail and other purposes, passwords must never be shared with or revealed to others. Users should not disclose passwords to administrative staff or to managers, even when requested to do so – the password for a user account is not required for administrative purposes and any request for your password should be viewed as suspicious. The exception to this is the `Administrator' or `root' password, which is shared by users who require special access. Sharing a password (or any other access mechanism such as a dynamic password token) exposes the authorized user to responsibility for actions that the other party takes using the disclosed password. If a service user believes that someone else is using his or her user-ID and password, the service user must immediately notify the administrator for the information system in question. If a password is discovered written down in an easily accessible location (for example on a whiteboard, or written on a sticky note attached to the bottom of a keyboard) the account will be treated as if it had been disclosed and will be disabled.

Multi-Factor Authentication

The implementation of Multi-factor authentication is highly encouraged whenever applicable not only for work accounts but for personal accounts too.

Privileged User-IDS and Passwords: Certain privileged accesses on production systems require the use of the administrative or Super-User (root) accounts. Knowledge and use of such user-IDS shall be restricted to a need-to-know basis. All users granted such access shall have their names added to the authorized administrative user list and shall be removed when access is no longer required. If a privileged user-ID/password has been determined to be compromised, then the scope of the compromise must be assessed and all passwords relating to the compromised system must be changed as appropriate.

Password Policy Conformance Auditing: From time to time the Information Technology Department or the Security Team may audit the multi-user computer systems for password policy conformance. If a password is not long enough (16+ characters) or does not contain enough special characters or is based on a dictionary word and is easily guessed, the account related to the weak password will be required to choose a more secure password. Audits may also include checking the vicinity of one's workspace for passwords that have been written down (sticky note on keyboard) but will not include a search of personal effects or within desk drawers.

Password Account Blocking: After six consecutive login failures an account will be blocked from further access for a minimum of 30 minutes (not including Network Infrastructure). If a user has had an account disabled in such a manner, they must contact the Information Technology Helpdesk following the IT Support Request Process to have the account re-enabled if it is necessary for the account to be accessible within the lockout time frame.

Violations of Password Policy: In the event that a password has been disclosed, either by accident or by the negligence of a user, the account in question must be disabled. In order for a service user to regain access to computing resources, an internal ticket request must be submitted by the user's manager before the account may be re-enabled for their use. Repeated violations or disclosure of access control information to an outside party will result in disciplinary action up to and including termination of employment. If your account has been disabled or you suspect that it has been disclosed, please immediately contact the Help Desk (ithelp@u32.org)

Acceptable Use Policy

Overview

WCUUSD’s intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to WCUUSD’s established culture of openness, trust and integrity. IT is committed to protecting WCUUSD's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

The question of Internet safety includes issues regarding the use of the Internet, Internet-capable computing devices, and other electronic devices in a manner that promotes safe online activity for children, protects children from cybercrimes, including crimes by online predators and cyberbullying, and helps parents shield their children from materials that are inappropriate for minors. To promote the safe and appropriate online behavior of students and staff as they access material from the Internet, the district will use the following four-part approach. However, given the ever-changing nature of the Internet, the district cannot guarantee that a student will never be able to access objectionable material.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of WCUUSD. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations. Please review Human Resources policies for further details.

Effective security is a team effort involving the participation and support of every WCUUSD employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

Purpose

This policy applies to employees, contractors, consultants, temporary and other workers, including all personnel affiliated with third parties. This policy applies to all equipment that is owned and/or leased by WCUUSD.

Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct WCUUSD business or interact with internal networks and business systems, whether owned or leased by WCUUSD, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at WCUUSD and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with WCUUSD policies and standards, and local laws and regulation. This policy applies to employees, contractors, consultants, temporaries, and other workers at WCUUSD, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by WCUUSD.

Right to Search and Monitor – No Expectation of Privacy

To ensure compliance with WCUUSD internal policies as well as applicable laws and regulations, and to ensure service user safety, WCUUSD administration reserves the right to monitor, inspect, and/or search at any time all WCUUSD information systems. This examination may take place with or without the consent, presence, or knowledge of the involved service users. The information systems subject to such examination include, but are not limited to, electronic mail system files, personal computer hard drive files, voicemail files, printer spool files, fax machine output, desk drawers, and storage areas. All searches of this nature will be conducted after the approval of the Legal and Human Resources Departments.

All district-owned and personally owned Internet-capable devices in all district facilities accessing the Internet through district network resources will be filtered and monitored to prevent access to obscene, racist, hateful, violent, or other objectionable material as specified in the FCC Children’s Internet Protection Act or district policies.

Since WCUUSD's computers and networks are provided for business purposes only, service users should have no expectation of privacy associated with the information they store in or send through these information systems. WCUUSD administration additionally retains the right to remove from its information systems any material it views as offensive or potentially illegal. WCUUSD reserves the right to turn over potentially illegal material to law enforcement for civil and or criminal prosecution.

Internet Access / Acceptable Use for Personal Activity

Service users are generally provided with Internet access to perform their job duties, but this access may be terminated at any time at the discretion of a service user's supervisor. Service users must take special care to ensure that they do not represent WCUUSD in an official capacity on Internet discussion groups and in other public forums, unless they have previously received administration authorization to act in this capacity. All information received from the Internet should be considered to be suspect until confirmed by reliable sources; there is a great deal of inaccurate and deliberately misleading information available on the Internet. Separately, service users must not place WCUUSD material (software, internal memos, press releases, databases, etc.) on any publicly accessible computer system such as the Internet, unless both the information Owner and the Information Technology Department have first approved the posting. On a related note, sensitive information must not be sent across the Internet unless it is in encrypted form.

Supervision

When students and staff access the Internet from any district facility, district staff will make a reasonable effort to supervise student access and use of the Internet. If material is accessed that violates district policies, procedures and/or the network use agreement, then district staff may instruct the person to cease using that material and/or implement sanctions contained in district policies, procedures and/or the network use agreement.

Unbecoming Conduct

Prohibited Activities: Users must not test or attempt to compromise computer or communication system security measures unless specifically approved in advance and in writing by the WCUUSD IT Team or is specifically a part of their job duties. Incidents involving unapproved system cracking (hacking), password cracking (guessing), file decryption, bootleg software copying, or similar unauthorized attempts to compromise security measures may be unlawful and will be considered serious violations of WCUUSD internal policy. Likewise, short-cuts bypassing systems security measures, as well as pranks and practical jokes involving the compromise of systems security measures are absolutely prohibited.

Harassing or Offensive Materials: WCUUSD computer and communications systems are not intended to be used for and must not be used for the exercise of the service users' right to free speech. Sexual, ethnic, and racial harassment --including unwanted telephone calls, electronic mail, and internal mail -- is strictly prohibited and is cause for disciplinary action up to and including termination of employment. Service users are encouraged to promptly report the communications to their manager and the Human Resources Department.

WCUUSD retains the right to remove from its information systems any material it views as offensive or potentially illegal.

Appropriate Behavior: To avoid legal problems, whenever any affiliation with WCUUSD is included with an Internet message or posting, "flaming" or similar written attacks are strictly prohibited. Likewise, service users must not make threats against another user or organization over the Internet. All Internet messages intended to harass, annoy, or alarm another person are similarly prohibited.

Business Activities not Related to WCUUSD: It will be a violation of policy for any user to conduct business other than that of Washington Central Unified Union School District on WCUUSD Information Systems.

Electronic Mail

Overview

Electronic email is pervasively used in almost all industry verticals and is often the primary communication and awareness method within an organization. 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.

Policy

- All use of email must be consistent with WCUUSD policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.
- WCUUSD email account should be used primarily for WCUUSD business-related purposes; personal communication is permitted on a limited basis, but non-WCUUSD related commercial uses are prohibited.
- All WCUUSD data contained within an email message or an attachment must be secured according to the Data Protection Standard.

- Email should be retained only if it qualifies as a WCUUSD business record. Email is a WCUUSD business record if there exists a legitimate and ongoing business reason to preserve the information contained in the email.
- Email that is identified as a WCUUSD business 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 company'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.

Incident Response Policy and Plan

Overview

In accordance with security best practices, all security incidents will be formally documented and responded to. This policy provides some general guidelines and procedures for dealing with computer security incidents.

Purpose

The WCUUSD is committed to maintaining the security of electronic information. Formal practices of tracking and mitigating security incidents will aid in assessing potential risks and vulnerabilities to data. As such, WCUUSD will continually assess risks and improve security measures.

Incident Examples

Some examples of possible incident categories include:

- Compromise of system or data integrity
- Denial of system resources.
- Illegal access to a system (either a penetration or an intrusion).
- Malicious use of system resources
- Inadvertent damage to a system.
- Malware or virus detection.

Some possible scenarios for security incidents are:

- Loss of a laptop or device containing, HIPAA, PII and/or other WCUUSD – data.
- Suspicious activities or anomalies that are identified through intrusion detection, firewall or other network device logs. You have discovered a major virus has infected multiple systems.
- Damage, intentional or accidental, to equipment or system affecting its ability to perform its job.
- Unauthorized wireless access points.

Incident Reporting

All suspected policy violations, system intrusions, virus infestations, and other conditions which might jeopardize WCUUSD information or WCUUSD information systems must be immediately reported to the WCUUSD Information Technology Helpdesk (ithelp@u32.org), who will coordinate with the WCUUSD Director of Technology and/or Superintendent.

Confidentiality Agreements

Overview

WCUUSD expects that information disclosed to employees will be treated with the appropriate level of confidentiality; except as required by law, information concerning the organization’s business is not to be discussed with competitors, outsiders, or the media.

Purpose

To protect WCUUSD’S confidential information and that of the organization’s clients.

Employee Confidentiality Policy

Employees are prohibited from forwarding e-mails containing information on the organization’s business to anyone outside of WCUUSD or otherwise transmitting confidential information outside of the organization, whether over the Internet or otherwise. Failure to honor this confidentiality requirement may result in disciplinary action, which may result in termination of employment.

In the course of an employee’s work, employees will have access to WCUUSD confidential and/or proprietary information, including information concerning client’s (those who participate in WCUUSD programs and services) and suppliers, as well as fellow employees. It is imperative that no employees disclose such information in any inappropriate ways, and that such information be used only in the performance of regular job duties.

WCUUSD requires confidentiality or nondisclosure agreements from all staff and third-party staff not otherwise covered by third party contracts before access to sensitive information will be allowed.

This policy requires that staff sign confidentiality or nondisclosure agreements (unless otherwise contractually bound) prior to being granted access to any sensitive information or systems.

Agreements will be reviewed with the staff member when there is any change to the employment or contract, or prior to leaving the organization.

Terms and Conditions of Employment

WCUUSD will state the employee’s roles and responsibilities for information security in the terms and conditions of employment. All employees must clearly understand their responsibilities for maintaining and promoting security within WCUUSD during and subsequent to their employment as well as the sanctions for not doing so.

Human Resources will provide each new employee with the employee’s responsibilities for Information Security in the Employee Handbook. This handbook will contain information on Information Security policies, acceptable use, and ethics (direct information or instructions to obtain and read referenced policies).

The employee’s manager will provide the employee specific responsibilities that are particular to the specific position. At a minimum, all employees are responsible for information security and the protection of information and information assets.

APPENDIX A: Security References

The following references illustrate public laws which have been issued on the subject of cyber security and should be used to demonstrate WCUUSD responsibilities associated with protection of its cyber assets.

a. United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-53 Recommended Security Controls for Federal Information Systems Revision 4, Operational Controls, Configuration Management Control Family, January 2009.

b. United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-128 “Guide for Security Configuration Management of Information Systems” August 2011.

c. United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-70 Rev 4“National Checklist Program for IT Products – Guidelines for Checklist Users and Developers” August 2017.

d. United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-60 “Guide for Mapping Types of Information and Information Systems to Security Categories” Revision 1 August 2008.

e. United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-40 “Creating a Patch and Vulnerability Management Program” Revision 3 July 2013.

APPENDIX B: State Breach Notification Laws

Links to state breach notification laws.

State	Citation
Alabama	Ala. Code § 8-38-1 et seq.
Alaska	Alaska Stat. § 45.48.010 et seq.
Arizona	Ariz. Rev. Stat. § 18-551 to -552
Arkansas	Ark. Code §§ 4-110-101 et seq.
California	Cal. Civ. Code §§ 1798.29, 1798.82
Colorado	Colo. Rev. Stat. § 6-1-716
Connecticut	Conn. Gen Stat. §§ 36a-701b, 4e-70
Delaware	Del. Code tit. 6, § 12B-101 et seq.
Florida	Fla. Stat. §§ 501.171, 282.0041, 282.318(2)(i)
Georgia	Ga. Code §§ 10-1-910 to -912; 46-5-214
Hawaii	Haw. Rev. Stat. § 487N-1 et seq.
Idaho	Idaho Stat. §§ 28-51-104 to -107
Illinois	815 ILCS §§ 530/1 to 530/25, 815 ILCS 530/55 (2020 S.B. 1624)
Indiana	Ind. Code §§ 4-1-11 *et seq*., 24-4.9 *et seq.*
Iowa	Iowa Code §§ 715C.1, 715C.2
Kansas	Kan. Stat. § 50-7a01 et seq.
Kentucky	KRS § 365.732, KRS §§ 61.931 to 61.934
Louisiana	La. Rev. Stat. §§ 51:3071 et seq.
Maine	Me. Rev. Stat. tit. 10 § 1346 et seq.
Maryland	Md. Code Com. Law §§ 14-3501 *et seq.,* Md. State Govt. Code §§ 10-1301 to -1308
Massachusetts	Mass. Gen. Laws § 93H-1 et seq.
Michigan	Mich. Comp. Laws §§ 445.63, 445.72
Minnesota	Minn. Stat. §§ 325E.61, 325E.64
Mississippi	Miss. Code § 75-24-29
Missouri	Mo. Rev. Stat. § 407.1500
Montana	Mont. Code §§ 2-6-1501 to -1503, 30-14-1704, 33-19-321
Nebraska	Neb. Rev. Stat. §§ 87-801 et seq.

Nevada	Nev. Rev. Stat. §§ 603A.010 *et seq.*, 242.183
New Hampshire	N.H. Rev. Stat. §§ 359-C:19, 359-C:20, 359-C:21
New Jersey	N.J. Stat. § 56:8-161, 163
New Mexico	N.M. Stat. §§ 57-12C-1
New York	N.Y. Gen. Bus. Law § 899-AA
North Carolina	N.C. Gen. Stat §§ 75-61, 75-65, 14-113.20
North Dakota	N.D. Cent. Code §§ 51-30-01 et seq.
Ohio	Ohio Rev. Code §§ 1347.12, 1349.19, 1349.191, 1349.192
Oklahoma	Okla. Stat. §§ 74-3113.1, 24-161 to -166
Oregon	Oregon Rev. Stat. §§ 646A.600 to .628
Pennsylvania	73 Pa. Stat. §§ 2301 *et seq.*
Rhode Island	R.I. Gen. Laws §§ 11-49.3-1 et seq.
South Carolina	S.C. Code § 39-1-90
South Dakota	S.D. Cod. Laws §§ 20-40-19 to -26
Tennessee	Tenn. Code §§ 47-18-2107; 8-4-119
Texas	Tex. Bus. & Com. Code §§ 521.002, 521.053
Utah	Utah Code §§ 13-44-101 et seq.
Vermont	Vt. Stat. tit. 9 §§ 2430, 2435
Virginia	Va. Code §§ 18.2-186.6, 32.1-127.1:05
Washington	Wash. Rev. Code §§ 19.255.010, 42.56.590
West Virginia	W.V. Code §§ 46A-2A-101 et seq.
Wisconsin	Wis. Stat. § 134.98
Wyoming	Wyo. Stat. § 6-3-901(b), §§ 40-12-501 to -502
District of Columbia	D.C. Code §§ 28- 3851 *et seq.,* 2020 B 215
Guam	9 GCA §§ 48-10 et seq.
Puerto Rico	10 Laws of Puerto Rico §§ 4051 et seq.
Virgin Islands	V.I. Code tit. 14, §§ 2208, 2209

APPENDIX C: Washington Central Unified Union School District Breach Notification Letter Template

<<Name of WCUUSD Administrator>>
<<Title of WCUUSD Administrator>>
1130 Gallison Hill Road
Montpelier, VT 05602
Phone Number: 802-229-0553
<<Email of WCUUSD Administrator>>

<<Parent/Staff Name>>
<< Parent/Staff Address Line 1>>
<< Parent/Staff Address Line 2>>
<<PSN_City>>, <<PSN_State>>, <<PSN_ZipCode>>

Dear <<Parent/Staff Name>>:

We are contacting you because we have learned of a serious data security incident that occurred on (specific or approximate date) OR between (date, year and date, year) that involved some of your personal information.

The breach involved **(provide a brief general description of the breach and include how many records or people it may have affected).** The information breached contained (**names, mailing addresses, date of birth, HIPAA data such as diagnosis or disability codes, credit card numbers, and/or Social Security numbers, etc.).** Other information (bank account PIN, security codes, etc.) was not released.

We are notifying you so you can take action along with our efforts to minimize or eliminate potential harm. Because this is a serious incident, we strongly encourage you to take preventive measures now to help prevent and detect any misuse of your information. We have advised the three major U.S. credit reporting agencies about this incident and have given those agencies a general report, alerting them to the fact that the incident occurred, however, we have not notified them about the presence of your specific information in the data breach.

To protect you we have taken the following steps:
1.) Initiated a forensics security investigation into the incident
2.) Contacted law enforcement and opened a criminal investigation into the breach
3.) retained **(name of identity theft company)**, a specialist in identity theft protection, to provide you with 1 year of credit monitoring services, free of charge. You can enroll in the

program by following the directions below. Please keep this letter; you will need the personal access code it contains in order to register for services.

Your personal access code is **<<PERS_ACCESS_CODE>>**

As a first preventive step, we recommend you closely monitor your medical and financial accounts and, if you see any unauthorized activity, promptly contact Washington Central Unified Union School District immediately. We also suggest you submit a complaint with the Federal Trade Commission (FTC) by calling 1-877-ID-THEFT (1-877-438-4338) or online at https://www.ftccomplaintassistant.gov/

As a second step, you also may want to contact the three U.S. credit reporting agencies (Equifax, Experian and TransUnion) to obtain a free credit report from each by calling 1-877-322-8228 or by logging onto www.annualcreditreport.com. Even if you do not find any suspicious activity regarding your medical or financial information, the FTC recommends that you check your credit reports periodically. A victim's personal information is sometimes held for use or shared among a group of thieves at different times. Checking your credit reports periodically can help you spot problems and address them quickly. Also, this site is helpful when trying to determine next steps when personal information is compromised: AHIMA's Medical Identity Theft Response Checklist for Consumers: http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_039114.pdf

You also may want to consider placing an optional security freeze on your credit files. A freeze prevents an authorized person from using your personal identifying information to open new accounts or borrow money in your name.

You will need to contact the three U.S. credit reporting agencies to place the security freeze. The fee is $10 for each credit reporting agency. The agencies may waive the fee if you can prove that identity theft has occurred. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze.

To obtain a security freeze, contact the following agencies:

Equifax: 1-888-298-0045; web: www.freeze.equifax.com
TransUnion: 1-800-680-7289; web: www.transunion.com (search for security freeze)
Experian: 1-888-EXPERIAN; www.experian.com/freeze.com

If you have questions or concerns, you may contact us at this special telephone number: 802-229-0553. You can also check our website at https://wcsu32.org for information.

Sincerely,

<<Name of WCUUSD Administrator>>