

**WHITMAN COUNTY**  
*Department of Public Works*

Mailing Address:  
P.O. Box 430  
Colfax, WA 99111-0430

Administration/Engineering  
Road Maintenance  
Equipment Rental & Revolving  
Solid Waste Division  
Planning Division  
Building & Development

PHONE: (509) 397-6206  
Fax: (509) 397-6210

N. 310 Main  
2nd Floor Public Service Bldg.  
Colfax, WA 99111

## Whitman County Public Works (WCPW)

### Public Records Act and Records Retention and Management Memo – 09-01-2019.0

You are a public employee. As such, everything you do when you conduct Whitman County business in any capacity is subject to the provisions of the “Public Records Act” and “Records Retention and Management” laws.

The Washington State Public Records Act is one of the strongest open government laws in the nation.

Employees should be aware that work-related records, including, but not limited to, texts and voice messages on portable electronic devices, are public records subject to the Public Records Act. Employees have a duty to maintain such records in accordance with Washington Local Government Record Retention Schedules.

### Personal Computer Use – 09-01-2019.1

WCPW does not permit personal computers to connect to the Whitman County networks.

### Portable Electronic Device Use – 09-01-2019.2

#### Situation 1

**Employee has requested the use of and has been granted the use of, or is required to have, an employer issued digital camera, tablet, cellular phone/smart phone or VOIP phone number.**

Whitman County business may only be conducted on these devices that are within the uses allowed by County Policy. These uses include sanctioned applications, digital photography and videography, text messaging, voice calling, work related internet usage, voice messages and email communications.

Sanctioned Applications: Applications installed and setup by WCPW.

Digital Photography and Videography: When these features are used on any WCPW issued portable electronic device, the photos and video produced must be downloaded to a WCPW system for long-term backup and retention. The portable electronic device itself may not be used to meet the records retention requirements.

Text Messaging: Text messaging for Whitman County business is limited to the default text messaging application on the device or the provided VOIP application. No social media platforms or chat applications such as, but not limited to, Twitter, Facebook, Facebook Messenger, Apple iMessage, Snapchat, etc. are permitted without prior authorization, that include assurance that precautions have been taken to meet the requirements of the applicable records and retention laws. Text Message archiving is maintained by WCPW for employer issued devices, in order to meet records retention requirements.

Voice Calling: In the event a records request requires a copy of call log records, WCPW will contact the phone service provider to acquire the available log records, as required by law.

Voice Messages: Voice messages for Whitman County business are not permitted on portable electronic devices. All voice messages shall be redirected through the county Voice Messaging System (through the office phone system). Voice messages are maintained according to the applicable records retention requirements.

Email Communications: Email communications conducted for Whitman County business, on a portable electronic device, is conducted through the Whitman County email servers. Email records are maintained according to the applicable records retention requirements.

## **Situation 2**

### **Employee elects to use a personal digital camera, tablet, cellular phone/smart phone or VOIP number.**

The "Public Records Act" and "Records Retention and Management" laws apply to Whitman County related business activities. If an employee elects to use a personal portable electronic device for Whitman County business, the records and retention laws still apply. Regardless of the device ownership, if you are conducting work-related activities, then these record and retention laws apply to the employee's device.

One of the most noted cases that has tested this is *Nissen v. Pierce County*, 183 Wn. App. 581 (2014).

In this case, Pierce County Prosecutor Mark Lindquist, attempted to argue that text messages from his personal device were not subject to the Public records Act (PRA). Below are a few excerpts from and related to the referenced decision.

#### **From MRSC**

*Significantly, the county and Lindquist argued that the state and federal constitutions "categorically prohibit a public employer from obtaining public records related to private cell phone use without consent." In rejecting this argument, the court emphasized:*

*The ability of public employees to use cell phones to conduct public business by creating and exchanging public records – text messages, e-mails, or anything else – is why the PRA must offer the public a way to obtain those records. Without one, the PRA cannot fulfill the people's mandate to have "full access to information concerning the conduct of government on every level."*

Reference: <http://mrsc.org/Home/Stay-Informed/MRSC-Insight/August-2015/Public-Records-Act-Alert-Text-Messages-Sent-or-Rec.aspx>

*Agency employees are responsible for searching their files, devices, and accounts for records responsive to a relevant PRA request, produce any public records (e-mails, text messages, and any other type of data) to the employer agency, and then the agency proceeds just as it would when responding to a request for public records in the agency's possession (reviewing each record, determining if some or all of the record is exempted from production, and disclosing the record to the requester.)*

Reference: <http://mrsc.org/Home/Explore-Topics/Legal/Courts/Washington-State-Court-Decisions.aspx>

*No Constitutional Privacy Rights in Public Records on Personal Accounts.*

*This statement may sound oddly familiar since the Supreme Court made a similar ruling in the 2015 Nissen v. Pierce County case, holding an official had no constitutional privacy rights in a public record on his personal cell phone. West v. Vermillion and City of Puyallup expanded the Nissen ruling, holding that employees and officials have no constitutional privacy rights—including those afforded by the U.S. Constitution (the First and Fourth Amendments) and the Washington State Constitution (article I, section 7)—in public records on their personal websites and personal email accounts.*

Reference: <http://mrsc.org/Home/Stay-Informed/MRSC-Insight/January-2017/PRA-Case-Law-Round-Up-for-2016.aspx>

The clear stance of these opinions is that “Public Records Act” and “Records Retention and Management” laws still apply when personal devices are used for work-related activities. Please note that you are personally responsible to comply with PRA requests, and are compelled to cooperate with WCPW in fulfilling them when needed.

### **Summary**

Whitman County currently has no policy to prohibit use of personal resources for Whitman County business. It is strongly recommended that when you are performing work-related activities that are subject to the “Public Records Act” and “Records Retention and Management” laws, you stay fully informed of what would be required of you to comply with the law. Choosing to ignore the law or to not comply with its provisions could have drastic consequences for Whitman County and the individual.

More information can be found at [SOS.WA.GOV](http://SOS.WA.GOV) & [MRSC.org](http://MRSC.org)

Related County Policies are included with this document and available through Human Resources.

**The following must be signed and returned to Brandon Johnson:**

- **Acknowledgement of Receipt**
- **The current Whitman County Email/Internet Acknowledgment Form**
- **For employees that remotely connect to the County Network, the current VPN Policy.**

**Effective Date:** 12/1/08**POLICY****Cancels:** Res. 062267**Approved by:** BOCC**See Also:** POL-005-IS; POL-1500-HR**Res. # 068879**

POL-0408-HR

OVERSEEING COUNTY E-MAIL AND  
INTERNET SYSTEMS

Unless otherwise stated in a union contract, this policy applies to all Whitman County employees and authorized agents.

**Definitions**

**E-mail:** Electronic mail. Messages and attachments sent from one computer to another via an electronic system.

**Internet:** Thousands of interconnected electronic networks.

**User:** Anyone who is authorized to use an e-mail account or access the internet via Whitman County property.

**1. Whitman County Encourages the Use of County Computer Equipment.**

Whitman County encourages the efficient and effective use of county computer equipment. It recognizes that the computer is a necessary tool for receiving and sending vital information in county business. In doing so, the county expects all internet and e-mail users to exercise common sense and discretion.

It also realizes that email and internet use has the potential to be abused. Therefore, Whitman County hopes to eliminate that abuse with the use of this policy.

**2. Web Email is Available.**

At the discretion of the Department Head/Elected Official, employees may be given access to web email through Information Services. Web email, although not always used through a county computer, is subject to all laws and policies pertaining to email use through county equipment. This includes, but may not be limited to, all policies, procedures and laws concerning email use, security, privacy and public disclosure.

**3. The Information Services Director, Other Department Heads and Elected Officials are Responsible for County Electronic Systems.**

The Information Services Director is responsible for the operation and maintenance of the County's electronic information system. This includes use of the internet and e-mail.

Department Heads/Elected Officials are responsible for the oversight and enforcement of this policy.

**4. E-Mail and Internet Access is for Business Purposes Only.**

E-mail and internet access is to be used for business purposes only. As such, it should be retained and treated as any other county record.

It is not uncommon for employees/agents to receive personal e-mails or occasionally look up personal sites on the internet. However, this practice must be kept to a minimum, be within legal regulations and not violate any part of this policy. Furthermore, employees should not be exploring personal internet sites where the public can view them doing so. Personal use of the internet and/or e-mail must be approved by the Department Head/Elected Official.

Employees shall not stream audio or video for non-work related purposes.

**5. County Computers are County Property.**

All county computers and their contents are the property of Whitman County. Therefore, all files sent via e-mail and downloaded from the internet or any other source are also the county's property.

It should be remembered that e-mail may be disclosed through public disclosure laws and rules of discovery in the case of a lawsuit. Confidentiality cannot be expected, except in the case of medical/legally confidential or privileged information. Users should not send highly sensitive, confidential or privileged material through the e-mail or internet.

Due to retention laws, Information Services strives to retain all emails for three years. All emails requiring retention longer than three years, such as public disclosure requests and data specific to each department, are the responsibility of the Department Head/Elected Official in accordance with RCW 40.14.010.

**6. Computers are Subject to Monitoring.**

An employee's/agent's rights while using county computers do not include privacy. Whitman County reserves the right to monitor, in any way, the computer activities of the employee/agent. It is the Department Head/Elected Official's responsibility to oversee e-mail and internet monitoring.

Furthermore, by using the county's computer, e-mail system, internet access and other equipment, the employee/agent knowingly and voluntarily consents to and acknowledges Whitman County's right to monitor its property.

Department Heads/Elected Officials may review computer content, internet histories and/or e-mail at any time. They may do so at the individual computer station or through the county's networking system. Information Services may perform monitoring if requested in writing by the Department Head/Elected Official. Human Resources may request the monitoring of an employee's computer if reasonable suspicion of a violation exists. The reasoning for such a request must be documented and may only be made if, after being notified of the suspicion, the Department Head/Elected Official refuses to investigate the allegations within thirty calendar days.

If, during the course of their duties, Information Services' employees discover questionable activity on an employee's/agent's computer, they shall immediately report the activity to the Information Services Director. The Director shall then contact the Department Head/Elected Official.

It is important to understand deleting an internet file from your computer does not necessarily mean it has been deleted from the system.

**7. Whitman County Prohibits Certain Uses of the Internet and/or Email.**

The following are internet and/or e-mail uses specifically prohibited by Whitman County:

- Commercial use: unless it is a core function of the department, any form of commercial use to benefit an individual or organization other than Whitman County.
- Copyright Violations: any use that violates copyright laws.
- Solicitation: the purchase or sale of personal items in violation of the county's solicitation policies.
- Harassment: any use that harasses, retaliates or discriminates against employees, vendors, customers and any other individuals.
- Downloading or uploading files or programs without the permission of the Department Head/Elected Official and Information Services. Files from the internet, or any other outside source, may contain a virus and must be scanned by virus detection software prior to use. The installation of programs shall be coordinated with Information Services.
- Viewing, distributing or downloading offensive or sexually explicit material: this includes, but is not limited to, pornographic material.
- Inappropriate language: includes obscenity, vulgarity, profanity or name-calling. It may also include expressions of ill will against individuals or groups.
- Politics: use for political purposes.
- Misrepresentation: the use of aliases is prohibited. Whitman County also prohibits the misrepresentation of an employee, a job description or county position.
- Misinformation/Confidential Information: the release of untrue and or confidential information regarding county business. This includes accessing, viewing or forwarding confidential information unless the user has the same privilege or confidence or has obtained permission from the original sender.
- Viewing/Downloading Non-Business Related Information without the permission of the Department Head/Elected Official: this includes viewing, downloading or any other method for retrieving non-County related information.
- Hacking or spamming.

- Streaming audio or video for non-work related purposes.

**8. Large Attachments Should be Avoided.**

Large e-mail attachments (over five megabyte) should be avoided. Other means of communicating the information should be used.

**9. Security is Vital.**

It is the responsibility of each e-mail and/or internet user to maintain a degree of security. For this reason, security features should be updated regularly.

Computer and e-mail passwords shall be changed at least once per year. They must also be changed in the event of employee turnover, a change in software, a breach of privacy or any other event that would put confidential information at risk. Passwords shall be at least eight characters in length and consist of a combination of upper and lower case letters, numbers and at least one special character (i.e. exclamation point, @ sign, etc.). They shall not contain any part of the employee's username or full name. Employees/agents should not share their password with others or access another's e-mail except when authorized by the Department Head/Elected Official. Nor should passwords be stored where unauthorized individuals may easily access the information (i.e. under keyboards, on the front of monitors, etc.).

Passwords shall be reported to the Department Head/Elected Official or his/her designee. That individual shall store those passwords in a secure, confidential location. The Department Head/Elected Official and designee shall be the only individuals with access to the password record.

**10. Violations of This Policy are Subject to Discipline.**

Violation of policy regarding internet and/or e-mail use may result in discipline up to and including termination. Violations shall be immediately reported to the appropriate Department Head/Elected Official or Human Resources.

Furthermore, internet and/or e-mail access may be removed from any employee due to violations of this policy as determined by the appropriate Department Head/Elected Official.

Contractors, consultants or other authorized agents who violate this policy may be banned from e-mail/internet use. Their contracts may be terminated as well.

Whitman County reserves the right to bring legal action for misuse of its e-mail and/or internet system.

# POLICY

Cancels: F8

Approved by: BOCC

See Also: Whitman Co. Code 2.40

Res. # 064276

**POL-1400-HR**

## **TELEPHONIC COMMUNICATIONS**

**This policy applies to all Whitman County employees and authorized agents.**

### **Definitions**

**Telephonic Devices:** Telephones, cell phones, phone cards, fax machines or other devices used to communicate via a wire or wireless line. This does not include internet access (See POL-0408-HR).

#### **1. Whitman County Owns and Provides Telephonic Devices.**

Whitman County provides telephonic devices such as telephones, cell phones, phone cards, and fax machines to its employees. The appropriate distribution and maintenance of such devices shall be determined by each Department Head/Elected Official and Information Services. Telephonic devices are the property of Whitman County.

Acquiring telephonic devices is the responsibility of the Department Head/Elected Official and Information Services. Devices must be purchased through the County's purchasing policies and procedures. They must also be inventoried and have a recorded log of who they are issued to. Purchases of County cellular phones must be forwarded from the Department Head/Elected Official to Information Services. IS will keep a log of what phones have been purchased and who they have been issued to.

When considering the purchase of telephonic devices, the Department Head/Elected Official must take in to consideration the following factors:

- Business need
- Cost of requested device compared to alternative communication options
- Expected level of employee need and usage
- Ability to fund the cost through the department's current budget

2. **Employees May Use Their Own Cellular Phones with the Approval of the Department Head/Elected Official.**

With the approval of the Department Head/Elected Official, employees may use their own cellular phones for business purposes. The employee is required to register his/her cell phone with the Department Head/Elected Official and sign a Personal Cellular Phone Agreement. The Department Head/Elected Official must then forward the registration and agreement to Information Services.

The cell phone bill will be paid by the employee and then turned in to the county for reimbursement of business calls only. The employee must submit a copy of the original bill along with any other documentation. It is the employee's responsibility to track which calls are business related versus personal. The billing must include the number, individual/organization, date and time of each call to be reimbursed.

The use of personal cellular phones is a privilege and not a benefit. Therefore, the employee must agree that the County may terminate the Personal Cellular Agreement at any time.

The County is not responsible for the damage, destruction or replacement of personal cellular phones. Therefore, the employee is responsible for the purchase, maintenance and repair of his/her personal cell phone and equipment. The employee must also pay for any installation charges and any equipment needed, which will remain the property of the employee.

3. **Telephonic Devices are for County Business Only.**

Devices provided by the County are for business use only. However, County code does allow for specific personal uses when appropriate. Those uses are as follows:

- Notifying the employee's family when he/she is required to work late;
- Notifying the employee's family of a schedule/shift change;
- If the employee is traveling outside of the County on business, he/she may notify family of his/her location and status on a daily basis; and
- Family members may contact County devices to notify employees of an emergency or other problem.

The calls listed above shall be made during one of the employee's break times. Personal calls determined to be inconsistent with this policy must be reimbursed by the employee.

4. **Whitman County Prohibits Certain Uses of Its Telephonic Devices.**

Whitman County prohibits the use of its telephonic devices for any of the following activities:

- Commercial use: unless it is a core function of the department, any form of commercial use to benefit an individual or organization other than Whitman County.
- Copyright Violations: any use that violates copyright laws.
- Solicitation: the purchase or sale of personal items in violation of the county's solicitation policies.
- Harassment: any use that harasses, retaliates or discriminates against employees, vendors, customers and any other individuals.
- Making or receiving calls of an offensive or sexually explicit nature: this includes, but is not limited to, pornographic calls and/or phone sex.
- Inappropriate language: includes obscenity, vulgarity, profanity or name-calling. It may also include expressions of ill will against individuals or groups.
- Politics: use for political purposes.
- Misrepresentation: the use of aliases is prohibited. Whitman County also prohibits the misrepresentation of an employee, a job description or county position.
- Misinformation/Confidential Information: the release of untrue and/or confidential information regarding county business. This includes calling or receiving confidential information, except as provided by law.

- Making or receiving non-business related communications, except as provided by law, this policy and/or a Department Head/Elected Official.
- Driving and speaking on the phone. Unless the phone contains a hands-free device, employees shall not conduct business over the phone while driving. This action creates a safety hazard and legal liability.

**5. Telephonic Devices are Not Private.**

Except for personal equipment and accessories, Whitman County owns all telephonic devices and their communications. Therefore, Whitman County reserves the right to monitor its telephonic activity and deduct reimbursable amounts from an employee's wages. By using the county's telephonic devices, the employee knowingly and voluntarily acknowledges and consents to such monitoring.

Employees should keep in mind that cellular transmissions and fax machines may be inadvertently heard or viewed by others. Therefore, discretion should be used when discussing confidential information.

Each employee is responsible for the prevention of theft and/or vandalism of County telephonic devices.

**6. Violators of This Policy are Subject to Discipline Up To and Including Termination.**

Violations of this policy must be reported to the Department Head/Elected Official immediately. Violators may be disciplined up to and including termination. The contracts of authorized agents may be terminated.

Whitman County reserves the right to bring legal action for misuse of its telephonic devices.

## **POLICY**

Cancels:

See Also: POL-01600,01620,0408-HR  
PRO-01500-1,01500-2,01500-3,  
01500-4-HR

Approved by: BOCC  
Res. # 063841

### **POL-01500–HR      USING ELECTRONIC INFORMATION**

**This policy applies to all Whitman County departments and employees.**

#### **Definitions**

**Protected Health Information (PHI)** – Employee/client information of a private nature, including demographic, financial, medical/health and social data related to healthcare. PHI is found in a variety of forms, including oral, electronic and printed material.

#### **1.      Whitman County Recognizes the Risks of Electronic Information.**

The County recognizes its responsibility to protect electronic information for its employees/clients in accordance with state and federal regulations. This protection must extend to electronic Protected Health Information (PHI) in accordance with the HIPAA Security Rule. Therefore, this policy shall act in close conjunction with policy POL-01600-HR Protecting Private Information and POL-0408-HR Overseeing County E-Mail and Internet Systems. This policy shall concern electronically used, stored and/or communicated information only.

Whitman County recognizes that security risks to electronic information include, but are not limited to the following areas:

- Hacking
- Theft
- Moving/sending information by mistake
- Using expired passwords
- Information left in plain view of the public
- Unauthorized employee access
- Unauthorized non-employee access
- Unauthorized use and/or changes of information

2. **Policies and Procedures Involving Private Electronic Information Shall be Reviewed and Updated in Accordance with Policy POL-01600-HR.**
3. **Department Heads/Elected Officials and Employees are Expected to Take Reasonable Steps to Protect Electronic Information.**

County employees shall conduct services and operations in such a way that electronic information is protected in accordance with legal mandates and all related privacy policies.

Department Heads/Elected Officials shall be responsible for ensuring that access to private electronic information is limited to only those employees who need it in conducting their daily operations. Department Heads/Elected Officials shall investigate and, if feasible, use firewalls, screensavers, virus protection, record amending procedures and passworded documents.

Passwords shall be created by each employee. They shall be changed at least once per year. They must also be changed in the event of employee turnover, a change in software, a breach of privacy or any other event that would put confidential information at risk. Passwords shall be at least eight characters in length and consist of a combination of upper and lower case letters, numbers and at least one special character (i.e. exclamation point, @ sign, etc.). They shall not contain any part of the employee's username or full name. Computer passwords shall only be shared in case of emergency. Information Services shall be immediately notified and shall change the password as soon as possible. Passwords for files or documents shall not be shared with others except when authorized by the Department Head/Elected Official. Nor shall passwords be stored where unauthorized individuals may easily access the information (i.e. under keyboards, on the front of monitors, etc.).

Passwords shall be reported to the Department Head/Elected Official or his/her designee. That individual shall store those passwords in a secure, confidential location. The Department Head/Elected Official and designee shall be the only individuals with access to the password record.

The public shall not have unsupervised access to electronic equipment containing private information. The monitors of such equipment shall be turned from public view.

Visitors and/or contractors with authorized access to electronic equipment shall wear identification tags stating their role and the authorizing party. Identification tags may be requested by the appropriate Department Head/Elected Official through the Human Resources Department. They must be worn throughout the duration of the visitor/contractor's work with the County. Each department shall keep a record of who they have authorized, how long and why.

The downloading or installation of programs must be coordinated and approved by both the Department Head/Elected Official and Information Services. It must also be in accordance with policy POL-0408-HR. Each Department Head/Elected Official and Information Services are responsible for ensuring that all software/hardware is installed properly, licensed correctly and protected from computer viruses. All malicious software must be immediately reported to the Department Head/Elected Official and Information Services (See procedure PRO – HR).

Employees shall not copy software belonging to others or the County. Nor shall they read another employee's files without the permission of the Department Head/Elected Official. Software shall be transported between computers only by Information Services and with the cooperation of the Department Head/Elected Official.

4. **All County Electronic Equipment Is Subject To Review and Monitoring.**

All electronic equipment and software provided by Whitman County is the property of the County and, therefore, subject to review and monitoring. Employees shall be held accountable for all usage of their systems.

5. **Each Department Shall Ensure That Only Authorized Personnel Have Access to Electronic Information.**

Authorized access to electronic information shall be governed by the Department Head/Elected Official in accordance with policy POL-1600-HR. Authorizations may come in the following forms:

- Specific written authorization for a specific time period (See procedure PRO – HR)
- Authorization written in to a position's job description
- Documentation required by policy POL-01600-HR
- Issued keys and/or pad lock combinations
- Documented department policy and/or procedure

All log-in attempts to County computers will be recorded and monitored on an as needed basis. Information Services shall assign each computer a user name in accordance with the employee authorized to use it (See procedure PRO – HR). Once an employee leaves employment, or no longer has a need to use a specific computer, the user name shall be disabled and/or changed to reflect the newly authorized individual (See procedure PRO – HR). User name assignments shall be recorded and tracked by Information Services.

Appropriate measures must be taken in order to protect electronic information after access is no longer needed. Such measures may include, but not be limited to:

- Changing door locks
- Changing security pad combinations
- Changing passwords to computers and files
- Voiding written authorizations allowing access to private information
- Amending job descriptions
- Amending documentation in accordance with policy POL-1600-HR

Repairs and modifications to the physical security components of County buildings shall be recorded by Facilities Maintenance.

All necessary records shall be changed to reflect the change in access within 60 days of the change's effective date.

6. **All Business Associate Agreements Shall Include Electronic PHI and be in Compliance with Policies POL-01600 & 01620-HR.**
7. **All Disclosures and Uses of Private Electronic Information Shall Be the Minimum Necessary in Accordance With POL-01600-HR.**
8. **Electronic Equipment No Longer Used Shall Be Cleared.**

Electronic equipment no longer in use or required for retention shall be cleared. Equipment such as disks, tapes, etc. containing private information shall be stored in accordance with POL-01600-HR and then destroyed. Computers shall be reformatted before being stored for future use and/or sold in accordance with County policy.

Information Services is responsible for assisting each department with securing private data before moving/destroying any electronic equipment. Records for the movement of hardware, media and those responsible shall be kept by Information Services (in cooperation with each department) via inventory controls and any other appropriate County policies.

9. **Whitman County Shall Provide Training to Its Employees In Accordance with Policy POL-01600-HR.**

County employees shall receive training in accordance with policy POL-01600-HR. In addition, equipment containing private electronic information shall be programmed to periodically remind employees to update their passwords and other security devices.

10. **In Case of Emergency, Information Services and Each Department Head/Elected Official Are Responsible For Data.**

In case of emergency, Information Services and the appropriate Department Head/Elected Official shall be responsible for retrieving lost data and securing it from unauthorized individuals. Access at the time of the emergency shall only be given to Information Services, the Department Head/Elected Official and individuals specifically authorized by the Department Head/Elected Official.

Policies and procedures for data contingency plans, evaluation, integrity and transmission security are the responsibility of Information Services. Employees who detect a problem must contact their Department Head/Elected Official and/or Information Services immediately.

11. **Misuse, Loss or Unauthorized Disclosures of Electronic Information Shall be Subject to Discipline.**

Misuse, loss or unauthorized disclosure of private information shall be subject to discipline in accordance with policy POL-01600-HR. Violations of the policy shall be immediately reported to the Department Head/Elected Official and Information Services. The Department Head/Elected Official, in cooperation with Information Services, shall keep a record of incidents and outcomes.

12. **PHI Documents Shall be Kept for Six Years.**

This policy shall be retained by Human Resources for at least six years past its expiration. This policy shall be available to all County employees and those charged with implementing its requirements. Furthermore, the County shall keep the following PHI documents for six years after their irrelevancy in accordance with HIPAA:

- Healthcare Plan documents

- Policies on PHI uses and disclosures
- Minimum necessary policies
- Signed authorizations
- Privacy Notes
- Documents regarding individual rights for the treatment of PHI
- PHI disclosures for purposes other than the regular treatment, payment or healthcare operations
- All complaints regarding PHI and their outcomes
- Sanctions imposed on violators
- Business Associate contracts

## **POLICY**

See Also: POL-0408-HR

### **POL – 0001-IS      VPN User Agreement Policy**

Definitions:

**VPN:** (Virtual Private Network) is a way to provide remote access to an organization's network via the Internet.

**VPN User:** Anyone authorized by Information Services and their Department Head / Elected Official to access Whitman County Network Resources remotely.

**Internet:** Thousands of interconnected electronic networks.

**Screensaver:** A program that displays an image, animation, or just a blank screen on a computer after no input has been received for a certain length of time.

**Domain:** A collection of computers and users that share common resources that are authenticated through a server.

**Remote Desktop:** A program provided by Microsoft to provide a remote connection to a computer running Windows XP Professional.

#### **1. VPN Security Guidelines**

1. You will not share your VPN User name and password with anyone except Information Services staff.
2. You will not allow anyone except yourself to access Whitman County Network Resources. (Files, Printers, E-Mail, Databases and any other resource that can be accessed via the Whitman County Network.)
3. You will take reasonable measures against unauthorized access to the VPN.
  - a. Log out of the Whitman County Network if you leave your computer unattended for more than 10 minutes.
  - b. Use a screensaver password and set your screensaver to come on after 5 minutes of inactivity.

#### **2. Adherence to Policy POL-0408-HR**

Please refer to Section 6 of policy POL-0408-HR. This section is applicable to Whitman County E-mail accessed via the VPN.

**3. Personal Computer usage with the VPN**

It is preferred that a computer owned by Whitman County is used with the VPN. If this is not possible then a personal computer may be used. The personal computer will not be added to the Whitman County Domain. Users will use “Remote Desktop” to access their work computer through the VPN. Please be aware that any work or county files which you copy or move onto your personal computer are subject to public records request to the same extent as they would be if the file was in paper form and took it to your home.

**2. Violations of This Policy are Subject to Discipline.**

Violation of this Policy regarding VPN usage may result in discipline up to and including termination of VPN access.

Whitman County reserves the right to bring legal action for misuse of its e-mail / or internet system via the VPN.

I, \_\_\_\_\_, have read the VPN User Agreement Policy, as  
(Print Name) written above. I understand and agree to follow the guidelines it contains.

Employee \_\_\_\_\_ Date \_\_\_\_\_

Department Head /  
Elected Official \_\_\_\_\_ Date \_\_\_\_\_



## **Whitman County Email/ Internet Acknowledgement**

### **Email/Internet Policy**

I have received and read the Whitman County access to the email and internet and agree to abide by all rules concerning its use. I acknowledge that all policies, procedures and laws concerning email use, security, privacy, and public disclosure apply to web email access/ use just as they do to my office access.

I understand that copies of the policy and questions regarding its content may be directed toward the Human Resources Department.

Furthermore, I agree to abide by the policy's guidelines. I understand that a violation of the policy may result in discipline up to and including termination.

\_\_\_\_\_  
Print Employee's Name

\_\_\_\_\_  
Employee's Signature

\_\_\_\_\_  
Date

### **Web Access to Email Acknowledgement**

I understand that it is my Department Head/Elected Official's decision to provide me with web email access. Therefore, I acknowledge that my access may be removed and discipline may be invoked if I am found to have violated applicable policies and/or laws.

\_\_\_\_\_  
Print Employee's Name

\_\_\_\_\_  
Employee's Signature

\_\_\_\_\_  
Date

WHITMAN COUNTY  
*Department of Public Works*

Mailing Address:  
P.O. Box 430  
Colfax, WA 99111-0430

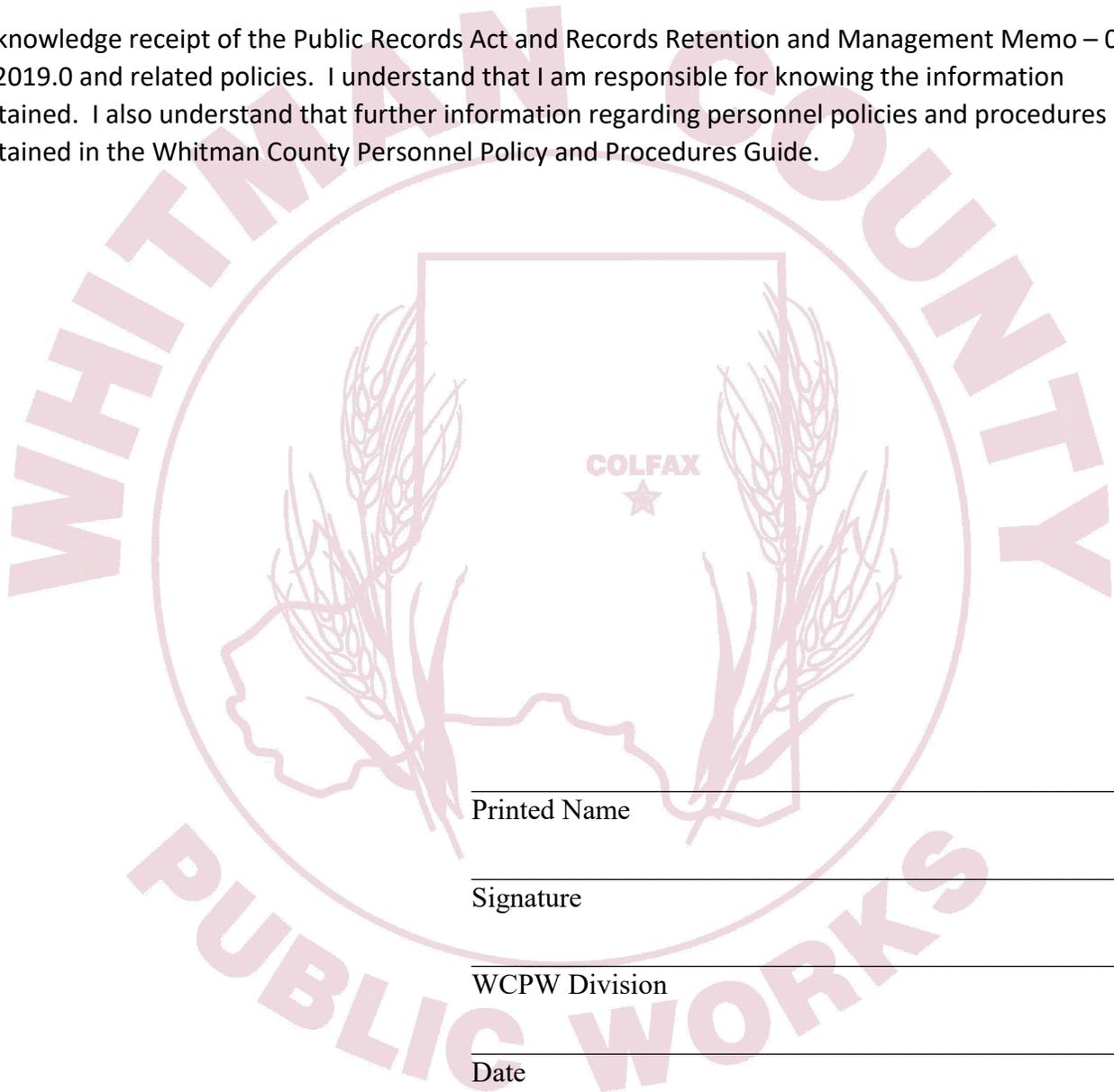
Administration/Engineering  
Road Maintenance  
Equipment Rental & Revolving  
Solid Waste Division  
Planning Division  
Building & Development

PHONE: (509) 397-6206  
Fax: (509) 397-6210

N. 310 Main  
2nd Floor Public Service Bldg.  
Colfax, WA 99111

**Acknowledgement of Receipt**

I acknowledge receipt of the Public Records Act and Records Retention and Management Memo – 09-01-2019.0 and related policies. I understand that I am responsible for knowing the information contained. I also understand that further information regarding personnel policies and procedures is contained in the Whitman County Personnel Policy and Procedures Guide.



\_\_\_\_\_  
Printed Name

\_\_\_\_\_  
Signature

\_\_\_\_\_  
WCPW Division

\_\_\_\_\_  
Date