BOARD OF COUNTY COMMISSIONERS
COUNTY OF KITTITAS
STATE OF WASHINGTON

RESOLUTION

NO.: 2013-_____

TO ADOPT A MOBILE DEVICE POLICY AND REVISED PERSONAL EQUIPMENT AND ENFORCEMENT POLICIES

WHEREAS: The Information Technology Department has established a set of Technology policies; and

WHEREAS: Resolution 2009-128 established (1) Introduction, and (6) Personal Equipment policies; and

WHEREAS: The Information Technology Department has written a (13) Mobile Devices policy and rewritten the (1) Introduction and (6) Personal Equipment policies; and

WHEREAS: The Information Technology Department has renamed the (1) Introduction policy to be (1) Enforcement to align with Criminal Justice Information Systems Security Policy 5.0 requirements; and

WHEREAS: The Information Technology Committee reviewed the policies in its August 13, 2013 meeting and recommends they be adopted by the Board of Commissioners; and

WHEREAS: The Management Team reviewed the policies in its August 14, 2013 meeting and voiced no concerns with the polices;

NOW, THEREFORE BE IT RESOLVED that the Kittitas County Board of Commissioners hereby adopts the attached Information Technology Policy 1 Enforcement, 6 Personal Equipment, and 13 Mobile Devices.

ADOPTED this 20 day of August, 2013.

BOARD OF COUNTY COMMISSIONERS
KITTITAS COUNTY, WASHINGTON

_____
Commissioner, Chair

Commissioner, Vice-Chair

Commissioner

ATTEST:
CLERK OF THE BOARD

Julie A. Kjorsvik

1. Enforcement

Adopted by the Board of County Commissioners on 8/20/2013

1.1 Summary

Computer information systems are an integral part of Kittitas County's daily operation. These policies have been approved by the Board of County Commissioners (BOCC) in order to:

- Maintain the systems used to provide services to the citizens of Kittitas County and protect the substantial human and financial resources invested to create and maintain these systems.
- Safeguard the information contained within these systems.
- Minimize business and legal risk.

1.2 References

- Personnel Policy Manual
- KCIT Policies
- Records management policy and procedures

You must adhere to the Kittitas County Information Technology (KCIT) policies and all related administrative policies including employee conduct and rights, records management, confidentiality, privacy, security of County technology assets.

1.3 Definitions

None.

1.4 Policy

1.4.1 Administration

The KCIT Director is responsible for the administration of the Information Technology policies.

1.4.2 Violations

If you violate KCIT Policies you may be subject to progressive discipline (including termination), revoked network access, and criminal investigation in accordance with Kittitas County policy and applicable laws.

1.5 Responsibilities

1.5.1 Department Head/Elected Official (DH/EO)

You are responsible for ensuring your staff is aware of and complies with these policies.

1.5.2 Employees

1. Understand and follow KCIT policies.
2. Ask your DH/EO, supervisor, or IT if you have any questions about this or any other policy.

1.5.3 Information Technology

1. Provide appropriate support and guidance to assist employees to fulfill their responsibilities under these policies
2. Enforce IT policies in a consistent and thorough manner
3. The IT Director shall develop and maintain written standards and procedures necessary to ensure implementation of and compliance with these policies.

6. Personal Equipment

Adopted by the Board of County Commissioners 8/20/2013

6.1 Summary

The County allows use of personal equipment to enhance productivity and safety. This policy sets requirements for using personal equipment to conduct Kittitas County (KC) business while maintaining the security of the network and public records.

6.2 References

- Personnel Policy Manual
- KCIT Policies
- Records management policy and procedures

If you use personal equipment for KC business, you must adhere to all related administrative policies including employee conduct and rights, records management, confidentiality, privacy, security of County technology assets.

6.3 Definitions

6.3.1 Mobile device

A smartphone, laptop, notebook, tablet, or similar device that includes an operating system and can run applications like e-mail, Internet access, and word processing.

6.3.2 Peripheral equipment

A mouse, keyboard, headphones, or other item that connects to a computer but does not have an operating system or store data.

6.3.3 Personal equipment

Any equipment (wired or wireless, including computers, tablet PCs, USB, Bluetooth, serial devices, flash memory, portable storage, MP3 players, wireless access points, routers, and other network devices,) not owned by the county, another government agency, or by contract through which county business is conducted.

6.3.4 Remote wipe

A process initiated outside of a mobile device that restores its configuration to the original—or factory default—state. A remote wipe will remove all the data, settings, and apps you installed.

6.4 Policy

6.4.1 Authorization

Before you can connect personal equipment to any County system, you must first get approval from your Department Head/Elected Official (DH/EO) and the IT Director using the Personal Equipment Authorization Form (see CAMAS > Forms & Policies > Forms > Technology).

6.4.2 Public records

If you use personal equipment to conduct county business, you might be required to produce equipment and phone records for public disclosure requests. If a court order is served, your equipment may be searched and/or seized with or without your knowledge or consent.

You may not store sensitive, confidential, or proprietary KC data on personal equipment.

All primary records must reside on the network (see KCIT Policy 7 Data Management, Access, and Protection).

If you are uncertain what any of this means or have any questions, see your Records Manager/Public Disclosure Officer. For more information see the records management policy and procedures.

6.4.3 Equipment support

KCIT provides support only for connecting authorized personal equipment to Exchange Active Sync (EAS). KCIT will not provide training on how to use personal equipment; you will need to contact the manufacturer or vendor for operating instructions.

6.4.4 Safety

It is your responsibility to use the equipment prudently to ensure your safety and the safety of your co-workers and the public. See the KC Personnel Policy Manual 4-12 Technology Use for information on using mobile devices while driving a vehicle.

6.4.5 Public Wi-Fi

In certain areas of KC buildings, public Wi-Fi is provided. It is separate from our KC network.

You can connect personal equipment the Internet over Wi-Fi using the ***Kittitas County Public*** connection.

6.4.6 Attaching personal equipment to the network

- You may connect your personal smartphone that has been authorized to sync with Exchange to your computer for battery charging only.
- You may connect personal peripheral equipment to your computer.
- You may not connect other personal equipment, directly or using VPN, to the KC network or to computers connected to the network.

Your DH/EOs may request IT give you remote access to your KC computer using a KCIT approved remote desktop solution.

6.4.6.1 Vendor and visitor owned equipment

Vendors may connect to their equipment via VPN. See KCIT Policy 5 Access.

6.4.6.2 Visitor owned equipment

Visitors may connect to the Internet via designated guest ports or over Wi-Fi using the ***Kittitas County Public*** connection. They may not connect to the KC network.

6.4.7 Email

With DH/EO approval, KCIT will sync your mail-enabled personal equipment with Exchange for email, contacts, and calendars. Email primary records are stored in KC's Exchange Server.

If your personal equipment is connected with EAS, you must follow these rules:

1. Follow records management policy and procedures.
2. Check for and install security updates as they are made available by the manufacturer.
3. Password protection must be enabled and required after 15 minutes of inactivity. Whenever possible the password must meet the requirements in KCIT Policy 4 Account Management.
4. Do not share your password with anyone, including family, co-workers, and KCIT.
5. You must change your device password every 90 days. We recommend you make this change when you change your County network password.
6. Report lost or stolen devices—as soon as the loss is noticed—to your DH/EO regardless of time, day or night. DH/EOs must notify IT staff or the IT Director as soon as notified by their employee. KCIT will immediately remote wipe lost or stolen devices.
7. Do not let your device store passwords automatically.
8. If you separate from service, you must visit IT to have your KC email sync disabled and the email removed from your device. If you do not KCIT may wipe your personal phone.
9. You connect to the county network at your own risk and KC is not responsible for any damage to your device.

KCIT will register all devices connecting to EAS for KC email.

6.4.8 Smartphones and Tablet PCs

Smartphones and tablet PCs must meet the following standards:

1. Managed by EAS software which provides a remote data-wipe capability
2. Operate on Windows Mobile 6.1 or higher, Android version 2.2 or higher, or Apple IOS 4 or higher

Best Practice Tip

Activate a find my phone feature if available.

Include return to information, e.g. your name and a contact phone number, on the device lock screen wallpaper.

See the KC Personnel Policy Manual 4-12 Technology Use for cellular phone policies.

6.4.9 Portable storage devices

Portable storage devices include smartphones, laptop and tablet computers, flash (USB) memory, MP3 players, and portable hard drives. They expose the county to security risks such as:

- Loss/misplacement/theft of device and data
- Viruses and malware
- Multiple copies of documents creating possible version conflicts; see KCIT Policy 7 Data Management, Access, and Protection
- The possibility for third parties to reconstruct files after they have been deleted.

You may not connect personal portable storage devices to any PC or other device connected to the county network. If you need to transport records, a KC owned portable storage device must be used. For more information, see KCIT Policy 7 Data Management, Access, and Protection.

6.4.10 Repairs

As an employee of the county, IT staff will not work on an employee's personal computer or equipment except for minimal phone troubleshooting for issues relating to remote access.

As an independent contractor, IT staff may not work on an employee's personal computer or equipment for any issue related to county business (see KC Personnel Policy Manual 4-5 Outside Employment).

6.5 Responsibilities

6.5.1 Department Heads, Elected Officials, and their Designees (DH/EO/designee)

1. Ensure your staff is aware of and complies with these policies.
2. Authorize device connection to the KC network using the Personal Equipment Policy Authorization form, as needed for county business.
3. Report lost or stolen network connected personal equipment to IT staff or the IT Director.
4. Notify IT when employees who have network connected personal equipment separate from service.

6.5.2 Employees

1. Manage and encrypt records on your network connected personal equipment.
2. Understand how to use your personal equipment.
3. Immediately report lost or stolen network connected personal equipment to your DH/EO/designee.
4. Immediately report virus or malicious software detection on your network connected personal equipment to IT.
5. Keep your network connected personal equipment password protected, upgraded, and patched.
6. Use your network connected personal equipment safely and securely.

7. Ask your DH/EO, supervisor, or IT if you have any questions about this or any other policy.

6.5.3 Information Technology

1. Register and document all personal equipment connecting to the KC network and EAS.
2. Remote wipe any lost, stolen, or high risk separation mobile network connected personal equipment when notified.

6.6 Related Documents

- KC Personnel Policy Manual 4-5 Outside Employment
- KC Personnel Policy Manual 4-12 Technology Use
- KCIT Policy 1 Enforcement
- KCIT Policy 4 Account Management
- KCIT Policy 5 Access
- KCIT Policy 6 Personal Equipment
- KCIT Policy 7 Data Management, Access, and Protection

6.7 Enforcement

If you violate this policy you may be subject to progressive discipline (including termination), revoked network access, and criminal investigation in accordance with Kittitas County policy and applicable laws.

13. Mobile Devices

Adopted by the Board of County Commissioners 8/20/2013

13.1 Summary

This policy sets requirements for connecting mobile devices owned by Kittitas County (KC) to the KC network to access public records while maintaining the security of the network and public records. For personal equipment, see KCIT Policy 6 Personal Equipment.

13.2 References

- Personnel Policy Manual
- KCIT Policies
- Records management policy and procedures

If you use a KC-owned mobile device, you must adhere to all related administrative policies including employee conduct and rights, records management, confidentiality, privacy, security of County technology assets.

13.3 Definitions

13.3.1 Mobile device

A smartphone, laptop, notebook, tablet, or similar device that includes an operating system and can run applications like email, Internet access, and word processing.

13.3.2 Remote wipe

A process initiated outside of a mobile device that restores its configuration to the original—or factory default—state. A remote wipe will remove all the data, settings, and apps you installed.

13.4 Policy

13.4.1 Authorization

Before you can connect any device to the County network or any County system, you must first get approval from your DH/EO using the Mobile Device Policy Authorization form (see CAMAS > Forms & Policies > Forms > Technology).

13.4.2 Public records

Public records are anything documenting County business, so you need to preserve any work you do on mobile devices. Those records are subject to public records requests. All primary records must reside on

the network (see KCIT Policy 7 Data Management, Access, and Protection). If you are uncertain what any of this means or have any questions, see your Records Manager/Public Disclosure Officer.

13.4.3 Device support

KCIT will help you with your KC-owned Windows mobile device during normal business hours. We will help you:

- Select and purchase a Windows device
- Secure the device and set your password
- Install approved software (see devices below)
- Connect to the network and KC email

We recommend Windows devices. We do not recommend mobile devices running other operating systems and will only assist you connecting them to KC email.

Because of the variety of devices we will not be able to provide you training on how to use the device; you will need to contact the manufacturer or vendor for operating instructions.

13.4.4 Use

Mobile devices are subject to the same protection and guidelines as desktop computers. See KCIT Policies and KC Personnel Policy Manual 4-12 Technology Use.

- You may not use KC-owned equipment to conduct personal business.
- You must immediately return the device to IT if you determine it is no longer necessary, if you leave County employment, or if requested by IT for inspection or return. If you are unable to return the device by the deadline provided you may be required to reimburse the County the cost of a replacement.
- You must store County records in an encrypted folder or hard drive. De-encryption information must reside with your supervisor and/or IT.
- You may only store and use sensitive, confidential, or proprietary data on a KC-owned mobile device if it is a transitory secondary copy. The primary record must be stored on the network.
- Violation of any local, state, or federal law; of any County policy; or for personal financial gain, is prohibited.

13.4.5 Security

KCIT will register all devices connecting to the KC network or to Exchange ActiveSync (EAS) for KC email.

You must immediately report virus or malicious software detection, or possible security violations to IT.

KCIT may monitor your activity on any KC-owned device.

As the custodian of the device, you must regularly check for and install security updates as they are made available by the manufacturer.

KC-owned mobile devices must have a County asset tag in an easy to see location.

13.4.5.1 Passwords

Password protection must be enabled and required after 15 minutes of inactivity. Whenever possible the password must meet the requirements in KCIT Policy 4 Account Management. You must change your device password every 90 days.

> **Best Practice Tip**
>
> Change the security password on your mobile device when you change your network password.

13.4.5.2 Lost or stolen devices

You are responsible for protecting mobile devices provided to you from theft, loss or damage.

You must immediately report lost or stolen devices—as soon as the loss is noticed—to your DH/EO regardless of time, day or night. DH/EOs must notify IT staff or the IT Director as soon as notified by their employee. KCIT will immediately remote wipe lost or stolen devices.

13.4.6 Safety

The County entrusts employees with communications equipment to enhance productivity and safety. It is your responsibility to use the equipment prudently to ensure your safety and the safety of your co-workers and the public. See the KC Personnel Policy Manual 4-12 Technology Use for information on using mobile devices while driving a vehicle.

13.4.7 Wi-Fi

You may *not* use non-County Wi-Fi hotspots unless they are secured with encryption, e.g., WPA and WPA2.

13.4.8 Smartphone

Smartphones must meet the following standards:

1. Managed by Exchange ActiveSync software which provides a remote data-wipe capability
2. Operate on Windows Mobile 6.1 or higher, Android version 2.2 or higher, or Apple IOS 4 or higher

Use discretion when making sensitive or confidential calls as cell phone calls are not secure.

You may not *jail break* or *root* KC-owned mobile devices.

Do not download games, ringtones, etc., or non-work related applications to KC-owned devices.

You must activate a *find my phone* feature if available.

> **Best Practice Tip**
>
> Include return to information, e.g. your name and a contact phone number, on the device lock screen wallpaper.

For more requirements for using smartphones, see KC Personnel Policy Manual 4-12 Technology Use.

13.4.9 Laptops and tablets

We recommend Windows laptops and tablets.

Do not download games, ringtones, etc., or non-work related applications to KC-owned devices.

13.5 Responsibilities

13.5.1 Department Heads, Elected Officials, and their Designees (DH/EO/designee)

1. Ensure your staff is aware of and complies with these policies.
2. Authorize device connection to the County network using the Mobile Device Policy Authorization form, as needed for county business.
3. Approve equipment recommended by IT.
4. Report lost or stolen devices to IT staff or the IT director.

13.5.2 Employees

1. Manage and encrypt records on your mobile device.
2. Understand how to use your mobile device.
3. Do not use KC-owned equipment to conduct personal business.
4. Immediately report lost or stolen devices to your DH/EO/designee.
5. Immediately report virus or malicious software detection to IT.
6. Return your mobile device to IT when you no longer need it, separate from service, or if IT requests it.
7. Keep your mobile device upgraded, and patched, password protected.
8. Use your mobile device safely and securely.
9. Ask your DH/EO, supervisor, or IT if you have any questions about this or any other policy.

13.5.3 Information Technology

1. Register and document all devices connecting to the KC network and EAS.
2. Remote wipe any lost, stolen, or terminated employee mobile device when notified.
3. Wipe any mobile device returned to IT.
4. Ensure mobile devices are tagged and inventoried.

13.6 Related Documents

- KC Personnel Policy Manual 4-12 Technology Use
- KCIT Policy 1 Enforcement
- KCIT Policy 4 Account Management
- KCIT Policy 6 Personal Equipment
- KCIT Policy 7 Data Management, Access, and Protection

13.7 Enforcement

If you violate this policy you may be subject to progressive discipline (including termination), revoked network access, and criminal investigation in accordance with Kittitas County policy and applicable laws.