

Business Computer Equipment Policy - 02.01.05

Pierce County Information Technology Department

Policies, Standards and Procedures

Division:	IT Operations	Number:	02.01.05
Subject:	Standards	Title:	Business Computer Policy
Last Prepared By:	Dawn Umstot	Last Approved By:	County Executive John Ladenburg
Included:	<input checked="" type="checkbox"/> Policy <input checked="" type="checkbox"/> Standard <input type="checkbox"/> Procedure	Last Approval Date:	April 9, 2008

Purpose:

The purpose of this policy is to maximize business computer up-time and assure business continuity for Pierce County services by utilizing proven cost-effective best practices in computer technology support methodologies.

Definition of Terms:

Business Computer – Desktop PC’s, laptops, tablets, PDA’s, smartphones, BlackBerry devices and other similar user interface devices owned by Pierce County.

Business Computer Equipment – all the above plus peripheral equipment such as printers, plotters, digital cameras, web cameras, scanners, etc.

ISDB – Information Services Data Base; an application to track hardware and software inventory for Pierce County.

IT – the Pierce County Information Technology Department.

Security Software – software running on a computer whose purpose is to protect the computer from some security risk such as anti-virus protection, spyware protection, firewall protection, zero-day defense protection, etc.

Disk imaging software – software used to copy the entire contents of a computer’s hard drive.

Standard images –IT Operations configured and tested copies of computer hard drive images containing the established minimum starting configuration for each County standard business computer model.

Standard security software - Security related software centrally purchased by the IT Department to protect the County or a security related software standard mandated by the IT Department or the Information Technology Committee to run on devices to be funded by departments.

Policy:

Acquisition

Pierce County Purchasing Policy, as described in the ‘Budget & Finance Policy and Procedures Manual’, mirrors the Department of Information Technology purchasing policy which is that business computer equipment acquisitions require approval by the Information Technology Department (IT). This review is to assure compatibility with existing infrastructure investments, to utilize established standards and best practices to the benefit of county operations, and to save the County money. IT will concentrate its efforts towards providing responsive, cost effective support for County standard hardware and software. Occasionally IT will approve a non-standard purchase where no standard exists or where IT agrees there is benefit the County. In these cases, hardware and software support agreements will need to be determined prior to the purchase approval.

Maintenance

All business computer equipment repairs will be centrally provided through the County's [PC Lifecycle Program](#). Based on an approved formula, departments will contribute money from their annual budget to fund the [PC Lifecycle Program](#) and Information Technology will manage the contract and resources required to run this program. Maintenance for specialized devices such as plotters, high end scanners, and special servers will require separate maintenance contracts to be purchased and managed by the equipment owner. Please refer to the [PC Lifecycle procedures](#) (links to form) for more details on this program.

Best Practices for Desktop Management

All County business computers will follow these best practices adopted by Pierce County:

1. Business computer purchases must be one of the standard model choices or an alternative approved by the IT Operations division.
2. The operating system for each standard model will be determined by the IT Operations division. Without approval from IT Operations, this operating system will not be upgraded to any new version except for service pack releases.
3. Devices identified by the IT Operations division as capable of using disk imaging software will be setup using standard images as built and tested by the IT Operations division.
4. Devices identified by the IT Operations division as capable of running the County's standard security software will do so.
5. Devices identified by the IT Operations division as capable of running the County's standard desktop management tools will do so.
6. Wherever possible, devices will be configured to conserve energy through standard configuration settings or centrally controlled software managed by the IT Operations division.
7. Unless otherwise approved in advance by IT Operations division, only IT Operations staff or their designated department partners (DITS, LAN Managers) are allowed to install software on Pierce County business computers.

Software

Pierce County business computers will only run standard County software packages or other software developed or approved by IT. Pierce County employees may not use an alternate software package to meet their personal preferences.

Only software licensed to Pierce County and approved by IT can be used on Pierce County owned business computers. Exceptions would be software licenses being used under a valid evaluation program, a consultant legally using their software license on a County business computer in order to complete work for Pierce County, and other approved work related legal use of software licenses.

Software personally owned by Pierce County employees cannot be installed on Pierce County owned business computers. Ownership of personally owned software can be transferred to a Pierce County department following an established donation procedure that documents owner and department management approval (link to form).

Pierce County employees will comply with the terms and conditions of software license agreements and no employee may, or may be asked to, install duplicate copies

of software or other unlicensed software on business computers owned by Pierce County. IT will maintain proof of license ownership for all software licenses owned by IT for use on County computers. County departments are responsible for maintaining proof of license ownership for all software licenses they own and operate in their environment. These documents should be kept in an organized fashion, readily available for an auditor to access when a software compliance audit occurs.

Pierce County employees will not download or otherwise make copies of copyrighted software or other copyrighted materials without permission from the copyright owner. As such, downloading or copying of unlicensed software, music files, photographs, clipart, etc which violates copyright laws is explicitly prohibited.

Pierce County employees will not download or install any software, even if considered “free”, to Pierce County business computers without approval from IT. This includes entertainment and personalization software that employees may not see as licensed software needing approval. These programs often contain viruses, spyware, as well as other hidden threats; can interfere with the successful operation of legitimate County software used to run County operations; or can open a security risk to the entire County network. Employees need to be aware that breaking their business computer through personalization or personal software preference costs the County technical staff resource time to fix the problems caused by this usage. IT staff have been directed to report violations of this section of the policy to the employee’s management as well as the Human Resources Department.

Connectivity

County owned standard business computer equipment needing access to central systems from within County offices will be connected to the Pierce County internal network managed by IT according to their standards. Non-standard county owned business computer equipment can only be connected to the County network with written approval from IT. Computer equipment not owned by Pierce County will not be connected to the County network without a formal review by the IT Security Committee. Personally owned computer devices are expressly prohibited from being connected to the Pierce County internal network. Any device using a modem or multiple networking card configuration must be pre-approved by the IT Security Committee before it can be connected to the County network. IT reserves the right to immediately terminate any unauthorized or problematic network connection.

Asset Management

To comply with County Code, all business computer equipment purchased by the County will be entered into the [ISDB application](#) by IT Operations (following confirmation of equipment receipt through vendor report, packing slip or voucher payment). County departments are required to partner with IT Operations to maintain an accurate business computer equipment inventory through the use of the ISDB application. County departments will complete a physical inventory comparison to

ISDB once per year and report lost equipment per Budget and Finance procedures. County departments wishing to dispose of business computer equipment shall follow the [PC Lifecycle PC Disposal process](#).

Backups

Pierce County data should always be on centralized servers where data is safeguarded through backup processes. Non-server equipment (business computers, laptops) is not backed up because these devices can easily be re-built. Saving County data on local computer hard drives is not recommended. If an employee chooses to store County data on their local computer hard drive or other removable media the employee takes responsibility for safeguarding the data by performing routine backups.

Personal Use

Unless explicitly stated in a separate policy such as the [Email/Electronic Records Policy - 02.01.06](#) and [Internet Access/Use Policy - 02.01.16](#), employees are prohibited from using County business computer equipment for personal reasons. This includes creating personal use files, downloading software for personal enjoyment or preference, listening to music CD's or uploading music to the computer hard drive, watching entertainment DVD's, maintaining financial records, purchasing personal use items, etc. An acceptable exception is the use of a static personally owned photo for operating system wallpaper.

Other

The contents of County business computers are not private and can be reviewed at any time by County management or their representatives up to and including removal of the business computer for investigative purposes.

Please refer to the [IT Security Policy - 01.17.04](#) for additional requirements employees need to follow to securing the Pierce County electronic assets.

Standard:

Refer to Policy [02.01.11 - Standard Products for Application Development and Data Access](#).

Required security software: anti-virus software and zero day defense software. Required desktop management tools: patch management, software distribution, power savings software, remote support (unless denied by department director for security reasons) and inventory application software.

Procedure:

N/A

Method of Implementation:

N/A

References:

[IT Security Policy – 01.17.04](#)

Referral History:

Original Author:	Originally Approved by:	Original Approval Date:
Dawn Umstot, PC & Network Services Manager	Data Processing Management Committee	04/15/87
Revision made by:	Revision Approved by:	Revision Approval Date:
Dawn Umstot, IT Operations Manager **Note: This version supersedes all previous versions of the policy titled Personal Computer Policy (02.01.05)		4/9/2008

	Terry Hale, Director of IT	07/03/2006
	Information Technology Committee	01/11/2006
	County Executive John Ladenburg	07/03/2006

E-Mail/Electronic Records Policy - 02.01.06

Pierce County Information Technology Department

Policies, Standards and Procedures

Division:	Administration	Number:	02.01.06
Subject:	Documentation	Title:	E-Mail/ Electronic Records Policy
Last Prepared By:	Lew Sellers	Last Approved By:	ITC
Included:	<input checked="" type="checkbox"/> Policy <input type="checkbox"/> Standard <input checked="" type="checkbox"/> Procedure	Last Approval Date:	07/03/2006

Purpose:

To assure proper use of electronic records, including electronic mail ("E-Mail"), for authorized purposes by County employees within the parameters described in this policy.

Definition of Terms:

Electronic records

Any information transmitted or stored by electronic records means, including E-Mail messages; communications, and attachments that are sent or received by means of electronic mailing systems such as GroupWise, Microsoft's Exchange or E-Mail provided by a web browser.

Policy:

The County's electronic records systems are to be used primarily for Official County business purposes. The use for other than County business purposes is expected to be limited and restricted by the parameters provided within this policy.

Standard:

This Policy applies to all employees, or others, who use or may have authorized access to Pierce County's computer or E-Mail systems.

Procedure:

Personal Use of Electronic Records:

Occasional and incidental personal use of electronic records by authorized users may be permitted on a limited and brief basis where use of the system is not done in a manner that impacts work time or negatively affects the workplace. It is expected that such use will be conducted using good judgment and with the knowledge that we are accountable to the taxpayers. In addition, authorized users must understand that such use comes with the implicit and express consent of the user for the County to monitor, access, use and disclose electronic records. Such use must not violate other County policies (e.g., soliciting items for sale, harassment, Internet Access/use Policy, 02.01.16; use for private business, misuse of County time, etc.). See also “Prohibited Uses” in this policy. If an authorized user wants to send an E-Mail and they are uncertain about whether it is permitted under this policy, the matter should first be discussed with the supervisor.

Electronic Records Are Not Private:

The electronic mail and computer systems have been provided by the County to facilitate County communications and business. Electronic records are considered to be the same as any other County paper document and as such are the property of the County. The County reserves the right to monitor, access, use and disclose E-Mail and other electronic records. Additionally, unless those communications deal with matters exempted by state law, they are considered to be “public records” and not private or personal. As with all information contained on County computers/equipment, no one has a right to privacy in any matter created, received, stored, or sent on the electronic systems.

Extra care should be taken when communicating highly sensitive or confidential information or proprietary business information. In such cases, other, more secure means of communication should be employed to avoid any risk of disclosure, especially considering that electronic records sent over the Internet are usually sent in readable format by anyone on the Internet. You cannot control where an E-Mail may be forwarded. Once sent an E-Mail usually cannot be retracted. Even after an E-Mail is “deleted”, it is usually still possible to retrieve that E-Mail.

Electronic Records Use:

Frequency for Reading E-Mail: In order to make E-Mail effective, users are to check their e-mail at least once per day and to respond as appropriate in a timely manner.

Global Messages: County-wide messages may only be used by the County Executive's Office, E-Mail Administrator, and other authorized individuals or groups approved by the County Executive's Office, and only for Executive-sanctioned

purposes. Requests for global messages should be forwarded to the Executives Office.

Managing Disk Space: Users are responsible for deleting their E-Mail and electronic records in a timely manner. E-Mail files on County backup tapes are currently held for only fourteen (14) days. Information with no retention value (e.g., personal messages and announcements not related to County business, information only copies, and phone message slips) should be deleted immediately upon review.

Retention: Users are required to comply with the Public Records Retention Schedule and Destruction Authorization document (attached) and/or the Public Records Retention Schedule for their particular department's or tasks.

Prohibited Uses of Electronic Records:

The following are provided as examples of prohibited uses and are not intended to be all inclusive. Users are prohibited from sending, accessing, downloading, viewing, receiving, or possessing materials which would generally be considered to be inappropriate in the workplace. This includes any material of a sexual nature such as jokes, posters, pictures or sexual communications. In addition, communications which would be inappropriate under other policies are also prohibited (e.g., sexual harassment, racial comments, religious or political solicitations, insubordination, breaches of confidentiality, dealing with illegal activity, etc.) Other examples of prohibited uses include: use for personal or commercial gain, chain-letters, sending junk mail, bypassing security systems, attempting to cause harm to another computer system, actions which violate copyright or trademark laws or other license restrictions. Users are responsible for notifying individuals from whom they receive inappropriate or excessive E-Mail to immediately discontinue such use of the system.

Users who are unable to resolve unsolicited or inappropriate E-Mail themselves, should immediately notify supervisor or E-Mail administrator when receiving unsolicited, inappropriate E-Mail so they can assist in preventing such communications.

Users are prohibited from creating automated forwarding rules that send received emails to an external email address. Forwarding emails in this manner creates excess traffic on our Internet Server and may cause confidential or other sensitive County information to be transmitted and stored in an unprotected manner, outside our organization. Occasional forwarding of an individual, non-sensitive email message is permitted on a limited basis as long as it does not impact work time, negatively affect the workplace, or put sensitive data at risk.

The County shall consider a variety of factors when determining if there has been prohibited use of the County's computer system including, but not limited to the: 1) extent of use; 2) frequency of use; 3) sites accessed, 4) parties corresponded with; 5)

time spent; 6) impact or potential impact on the County; 7) potential risk of exposure to the County; 8) content or purpose of the message.

Disciplinary Action for Misuse:

The County considers misuse of its computer system to be a serious matter. Failure to follow this policy may be grounds for disciplinary action, up to and including discharge.

Method of Implementation:

N/A

References:

[Electronic Records 14-day Backup Cycle - Memorandum from John Ladenburg, County Executive, dated 1/14/2002](#)

[Public Record Retention Schedule](#)

[Internet Access/Use Policy - 02.01.16](#)

Referral History

Original Author:	Originally Approved by:	Original Approval Date:
Dawn Umstot	R.H. Trenbeath	08/13/91
Revision made by:	Revision Approved by:	Revision Approval Date:
Lew Sellers	<hr/> Terry Hale, Director	7/3/2006
Dawn Umstot	Information Technology Committee (ITC) Betsy Sawyers, Director Human Resources Terry Hale, Director Information Services	11/11/04
Personnel and Information Services	Information Technology Committee (ITC) Betsy Sawyers, Personnel Director Terry Hale, Information Services Director	03/31/04

Dawn Umstot	DPMC & Terry Hale, Director Information Services	04/10/97
-------------	---	----------

Internet Access/Use Policy - 02.01.16

Pierce County Information Technology Department

Policies, Standards and Procedures

Division:	Administration	Number:	02.01.16
Subject:	Documentation	Title:	Internet Access/Use Policy
Last Prepared By:	Dawn Umstot	Last Approved By:	County Executive John Ladenburg
Included:	<input checked="" type="checkbox"/> Policy <input type="checkbox"/> Standard <input type="checkbox"/> Procedure	Last Approval Date:	01/11/2007

Purpose:

The purpose of this policy is to define allowable and appropriate uses of the Internet.

Definition of Terms:

Business Computer – Desktop PC’s, laptops, tablets, PDA’s, smartphones, BlackBerry devices and other similar user interface devices owned by Pierce County.

Business Computer Equipment – Refers to all the above plus peripheral equipment such as printers, plotters, digital cameras, web cameras, scanners, etc.

Policy:

Internet Access

Filtered and logged Internet access is available to any user on the County's internal network by default. A Department Director or their designee can explicitly deny Internet access for a particular user or computer by request to the Information Technology Department. To enable certain specialized job functions, a Department Director may authorize, in writing to the Information Technology Department, unfiltered Internet access for particular employees.

Access to the Internet from any business computer connected to the County's internal network is only allowed via the County's centralized Internet connection. Alternate

methods of Internet access, such as using a modem to access America On-Line, would compromise the County's network security exposing it to potential harm. Requests for exceptions to this rule must be reviewed and approved by the Information Technology Department Security Committee.

Internet Use

All Pierce County employees are responsible for using Internet resources in an ethical, responsible and legal manner. The primary use of the Internet via Pierce County business computers will be for County business related purposes. Department Directors are responsible for managing use of the Internet by their staff, restricting use or limiting time as they see appropriate. Users should consider their Internet activity as public information and manage their activity accordingly. All Internet traffic goes out beyond the protected Pierce County network into a wide reaching un-secure network. The Information Technology Department monitors and reports on the Internet activity on the County's network.

Personal Use

As a benefit to employees, Internet access for personal use by authorized users may be permitted on a limited and brief basis where use of the system is not done in a manner that impacts work time or negatively affects the workplace. It is expected that such use will be conducted using good judgment, with the knowledge that we are accountable to the taxpayers and that personal Internet access directly competes for limited resources used to conduct legitimate County operations and provide the public access to our on-line government services. Employees will be held responsible for their Internet usage.

This limited personal use of the Internet is intended to allow employees incidental, unplanned, but necessary access to information needed during the workday, similar to the use of a County phone to make a brief personal phone call. These access periods are intended to be quick, as in less than five minutes, and to be specifically targeted activities rather than just looking around the Internet to pass the time on break. Such activities may not be done during work time. Please refer to the more detailed [**“Frequently Asked Questions: Personal Internet Use”**](#) document referenced later in this policy for more information.

Authorized users must understand that such use comes with the implicit and express consent of the user for the County to monitor, access, use and disclose activity. Such use must not violate other County policies (e.g., soliciting items for sale, discrimination, harassment, use for private business, misuse of County time, etc.). See also “Prohibited Uses” in this policy. If an authorized user wants to access an Internet site and they are uncertain about whether it is permitted under this policy, they should first read the [**“Frequently Asked Questions: Personal Internet Use”**](#) document referred to in the reference section of this policy matter. If questions remain, they should discuss them with the supervisor. Users must understand that all

personal use of the Internet via County resources is at their own risk and precautions necessary to protect their privacy and sensitive information is their responsibility.

Prohibited Uses

The following are provided as examples of prohibited uses and are not intended to be all inclusive. Users are prohibited from accessing, downloading, or viewing materials which would generally be considered to be inappropriate in the workplace. This includes any material of a sexual nature such as jokes, posters, pictures or sexual communications. In addition, communications which would be inappropriate under other policies are also prohibited (e.g., sexual harassment, racial comments, religious or political solicitations, insubordination, breaches of confidentiality, dealing with illegal activity, etc.) Other examples of prohibited uses include: use for personal or commercial gain, chat rooms, bypassing security systems, attempting to cause harm to another computer system, viewing or using bandwidth intensive activities, actions which violate copyright or trademark laws or other license restrictions. Employees are responsible for understanding what use is not acceptable and should read the [“Frequently Asked Questions: Personal Internet Use”](#) document referred to in the reference section of this policy.

The County shall consider a variety of factors when determining if there has been prohibited use of the County’s computer system including, but not limited to the: 1) extent of use; 2) frequency of use; 3) sites accessed, 4) parties corresponded with; 5) time spent; 6) impact or potential impact on the County; 7) potential risk of exposure to the County; 8) content or purpose of the message.

Standard:

N/A

Procedure:

N/A

Method of Implementation:

N/A

References:

Attachment: [Frequently Asked Questions: Personal Internet Use](#)

Revision History:

Original Author:	Originally Approved by:	Original Approval Date:
Dawn Umstot	Terry Hale	08/27/96
Revision made by:	Revision Approved by:	Revision Approval Date:
Dawn Umstot, PC & Network Services Manager	Terry Hale, Director of ISD	04/30/99
Dawn Umstot, IT Operations Manager	Terry Hale, IT Director Information Technology Committee County Executive John Ladenburg	07/03/2006
Dawn Umstot, IT Operations	<hr/> Terry Hale, Director of Information Technology	1/11/2007

Frequently Asked Questions: Personal Internet Use

Is personal use of the Internet allowed?

Yes. The County's Internet Access/Use policy (02.01.16) says "personal use by authorized users may be permitted on a limited and brief basis where use of the system is not done in a manner that impacts work time or negatively affects the workplace."

Why?

The County agrees to provide Internet authorized employees with this service as a benefit to address the occasional issue that arises during work where the Internet is the best method to handle it quickly. We are all busy people and we know this will help employees. We can offer this benefit as long as it is not abused in a way that negatively affects County operations or work time.

Are there limitations about what I can access for my personal use?

Yes, the County's Internet connection is **not** meant to provide your primary Internet access method for conducting personal business, reading news, completing on-line shopping, etc. As a rule of thumb, if the Internet access can wait until you are off work, then wait until then rather than tying up County resources for your personal business.

There are particular personal Internet activities which, even if quick, should be avoided to limit the negative impact on County operations. Specifically, bandwidth intensive activities and those with an accompanying security risk must be avoided.

Examples of bandwidth-impacting activities that should be avoided include:

- Viewing pictures and video on-line.
- Subscribing to web services that automatically send you updated information on a regular basis such as weather, sports scores or stock tickers.
- Transaction-oriented activity such as shopping, participating in on-line auctions, planning vacations and managing personal finances on-line.

As far as security risks go, accessing web pages including Internet Email can expose the County to risk of virus infection if you open up a web page that automatically executes a program or links to an infected file or attachment you choose to open. Please be cautious before opening any web page from an unknown source.

Any activity that violates other County policies, codes or guidelines is prohibited. In particular, employees should not access the Internet at work for any activity related to generating revenue such as running their own business.

I can use the phone on my desk for local personal calls, why are there more restrictions on personal Internet use?

There actually are some restrictions on the use of county telephones. For example employees must pay for personal calls on their county-owned cell phones and must pay for personal long-distance calls they make on their desktop phone. Personal Internet use cannot be billed to staff but because all Internet traffic coming in and out of the County goes through the same “pipe”, everything competes for the limited pipe size so we ask for your cooperation in limiting your personal use. While you are using the Internet at work for personal activity, you are sharing the limited bandwidth with the public looking to pay property taxes, private lawyers completing court activities on-line, employees using Internet resources to complete their work, partner agencies using our website information to help citizens, the public looking up court case information or permit status, etc. If you are connected to the Internet at home, you probably pay \$30-\$50 a month for this service. Internet connectivity for businesses is much more expensive. The County currently pays \$5,000 a month for our Internet pipe. I’m sure you can understand that we do not want to incur even higher costs so that employees can surf the Internet whenever and however they want.

What are examples of what I am allowed to use the Internet for personally?

Examples of acceptable personal Internet use:

- Obtaining directions from an on line mapping service to figure out how to drive by a particular store on the way home from work
- Checking the status of an incoming flight for someone you are picking up at the airport leaving directly from work
- Checking the loan rates at Tapco.com instead of making a phone call
- Looking up phone numbers; or checking the hours of a store you want to stop by on the way home.

This is by no means an all-inclusive list, but it gives you the idea that the County recognizes the value of the Internet as an information tool for busy working people that can make them more efficient overall.

Is there a better time to do this personal use?

Definitely! Please avoid using the Internet for personal use between 11 AM and 1 PM. This lunch hour time is our most congested period. Not only will your access be slower but so will the public’s and that of your County colleagues trying to do the County’s business.

What are some important considerations to remember if I do use the Internet for personal use?

All Internet access on County computers is logged. This information can be reviewed as part of an employee investigation. All personal use of the Internet via County resources is at your own risk and precautions necessary to protect your privacy and sensitive information are your responsibility.

What if I'm still unsure if a particular action is ok?

If this document has not addressed a specific question about whether a particular use is permitted under the Internet Access/Use policy (02.01.16), the matter should first be discussed with your supervisor.