SMITH COUNTY

INFORMATION TECHNOLOGY POLICY

Table of Contents

GOAL

In conjunction with the long range Smith County Information Technology Plan, it is the goal of this policy to achieve more standardization among computer hardware and software, copiers, telephones, and other equipment currently in use so that documents and data can be more freely transferred among departments. In addition, staff will gain expertise and efficiency in: (1) use and repair of hardware; and, (2) installation, maintenance and use of software.

USE AND SCOPE

This policy is intended to provide Smith County with a productive working environment that is consistent with Smith County policies and Federal/State laws. This policy applies to all Internet access, computer/network equipment and Smith County owned software. This policy will also apply to all computer users whether or not they are employees of **Smith County**.

Due to the rapidly changing nature of electronic media developing with on-line services, Internet, computer systems and networking technology, this policy cannot provide guidelines for every possible situation. It expresses general principles and guidelines for the use of Internet service, e-mail and computer/networking equipment by all **Smith County** departments.

The use of **Smith County** computers, network and communication devices must comply with Smith County policy and Texas law. **Smith County** computers, networking equipment or software cannot be used for commercial or profit-making purposes, for political campaigning, or for unsolicited mass distribution of religious, political, or non-County business-related materials. Furthermore, the transmission, receipt or storing of materials which federal or state law makes illegal to possess is strictly prohibited, and will be reported to the appropriate authorities.

All elected officials, department heads and employees are responsible for complying with this policy. Elected officials and department heads are responsible for enforcing and taking disciplinary action against employees in violation of this policy.

COMPUTER & COPIER PROCEDURE

All purchase orders for computer hardware and software, copiers, telephones, and other similar equipment in addition to the regular steps required by the Purchasing Policy, must also be routed through the Director of IT for both review and recommendation on the proposed purchase. **Any hardware, software, copiers, and other similar equipment that is not purchased through the IT Department will not be allowed connection to the Smith County network and will not be supported by the IT Department. The only exception to this will be with "the written authorization of the Smith County Judge, Department Heads only will be allowed to connect *supported* PDA's and cellular devices, they have personally purchased, to the Smith County network for email purposes.**

All requests for hardware purchases or upgrades must be sent to the CTO for approval. Upon approval the proposed request will then be routed to the Purchasing Department, who must approve all purchases. If the purchase is not approved, the purchase request will be send back to the Department Head with the reason(s) why. Anyone requesting hardware that is not considered standard will require written justification and approval by the Department Head.

Information Technology will maintain a hardware parts warehouse consisting of computers and replaced items from County computers if such items have any possible future use by other County departments. Whenever computers are replaced or whenever parts of computers

are upgraded, the IT Department will determine whether or not the part or computer being replaced is of no further value to the County or could be possibly be used by another department. If it could be used in the future, it will be transferred to IT for storage. If it is determined to be of no future use to the County, it will be transferred to Purchasing for disposal at the next County auction or donated to a nonprofit organization.

SOFTWARE

Information Technology is responsible for the installation and maintenance of all P/C Software. No software should be loaded onto any P/C unless installed by the IT Department (including Screensavers). It is illegal for any unlicensed software to be loaded on to a County P/C. **All new computers will be purchased with Microsoft XP-Pro.** The County wants to have a "core set" of uniform software being used so that a discounted "volume site license" can be obtained, and maintenance and upgrades standardized. All future County purchases of software will be subject to the following:

a. Must be in a M/S Windows-based environment;

b. Word processing must be done by Word (latest version);

c. Any requests to purchase software that does not use a Windows environment or word processing software that is not Word, must be accompanied by a written explanation of why the different software is required for that department's use and why the Windows or Word software is not satisfactory, and;

d. Each department that does not yet have a Windows-based software environment or which is not using Word for word processing should attempt through the budget process to migrate to this software as soon as possible.

IT will maintain a list of all county purchased software by department. All software must be properly licensed. Anyone caught loading unauthorized software will be locked out of access to the County network and appropriate disciplinary action taken.

COMPUTER USE/ETHICS

a. Contact the CTO when requesting a change of systems requirements for an associate. Upon hiring or termination of an employee, please notify the CTO.

b. Normally, two weeks advance notice should be provided so that there is enough time to properly plan and make network and phone system changes needed to facilitate.

c. County computers and computer networks are to be used only by full time, part time, temporary or contracted associates of Smith County, and *only for County purposes*.

d. No one shall give a computer password to an unauthorized person, nor obtain another person's computer password by any unauthorized means. No one except the System Administrator in charge of a computer is authorized to issue passwords for that Computer. Disclosing a password to an unauthorized person can be a crime under Texas law.

e. No one shall engage in, encourage, or conceal from authorities any "cracking," unauthorized tampering, or other unauthorized use or deliberate disruption of computers.

f. No one without specific authorization shall read, alter, or delete any other person's computer files or electronic mail, even if the operating system of the computer permits them to do so.

g. Users shall not place confidential data into computers without protecting it appropriately. The County cannot guarantee the privacy or authenticity of computer files or electronic communications unless special arrangements are made.

h. No one shall copy or use software or data in violation of copyright laws or license agreements.

i. Users shall take full responsibility for messages that they transmit through the County's computers and network facilities. Laws and rules against fraud, harassment, obscenity, and the

like apply to electronic communications no less than any other media.

j. Those who publish World Wide Web pages or similar information resources on County computers shall take full responsibility for what they publish; shall respect the acceptable-use conditions for the computer on which the material resides; shall obey all applicable laws; and shall not publish commercial advertisements without prior authorization. References and links to commercial sites are permitted, but advertisements, and especially paid advertisements, are not.

k. The departments approved for distribution of an email to all associates within the County will be Personnel, Commissioners Court, Physical Plant, and Information Technology. All other departments will be restricted from mass distributions of more than 20 email addresses. If a department requires an email to be mass distributed they should forward the requirement to the Personnel Department.

l. It is the Department Heads responsibility to ensure that their associates are using the resources according to these guidelines and are not abusing the standard software, including games, loaded on the computer.

INTERNET USE

The Internet connection you are using was established for business use. Use of this connection for non-business purposes is deemed an unacceptable use under this policy.

1. **Statement of Policy:** County-provided Internet access and electronic mail ("e-mail") are provided to assist employees and authorized users in the conduct of County business and are to be used only in an appropriate manner. The underlying principle is that County Associates will practice professionalism in their jobs and respect towards one another and persons outside the County with whom they come in contact. Appropriate personal use by employees of their Internet privileges and e-mail is permitted. **However, accessing inappropriate Internet sites (such as those that contain sexually-explicit, racial, hate, or gambling content), creating or forwarding e-mail containing inappropriate content, or spending excessive amounts of work time at non-business related sites are strictly prohibited. Employees that access inappropriate Internet sites will be subject to discipline as stated in the Personnel Policy, Section 4.-02 "Electronic and Technology Policy".** Employees should request guidance from their supervisor or the Technology Department on any questions regarding the business or personal use of their Internet or e-mail privileges.

2. **Employees must comply** with all County policies including, without limitation, the employee agreement (e.g., Confidential Information and Intellectual Property) and the Information Systems and Electronic and Voice Mail Policy. The content of all County computer systems is owned or licensed by the County and the County reserves the right to monitor or review the use and content of all such computer systems. **There is no expectation of privacy with respect to the use of County computer systems to access the Internet or with respect to the content of material sent to or received from the Internet on such computer systems.**

3. **Every user of Internet access and e-mail** must safeguard the intellectual property and proprietary information of **Smith County** and of third parties. Accordingly, care and discretion must be exercised when transferring information via the Internet or e-mail. In addition, when using e-mail County confidential proprietary information must be appropriately labeled, e.g., **"CONFIDENTIAL - PROPERTY OF SMITH COUNTY** not suitable for public disclosure must never be stored in publicly-accessible forums, such as newsgroups. Information retrieval from other sources on the Internet is allowed providing no proprietary third-party information is illegally or improperly transferred to County employees.

4. **Employees are responsible** for the security of their County Internet access and should

maintain their password and access numbers in a responsible manner. Employees should scan with virus checking software, when possible, all program executable files that are retrieved/received from the Internet or e-mail. Failure to adhere to this Policy can result in discipline up to and including discharge.

5. **Logs are maintained.** Policy requires that logs of browser access to the Internet be kept. These logs record when, where, and from what computer, Internet access has been allowed (or denied). Supervisors and authorized network management personnel have access to these logs.

6. **Non-business sites restricted.** In addition to keeping logs, the proxy software may also restrict access to certain sites that have been determined to have no valid business purpose, or have been determined to contain objectionable material. Attempts to access these sites will result in the display of this page.

7. **Exceptions made based on business need.** If you discover a web site that has been restricted, for which you have a business need, contact your supervisor and have them justify the access by submitting a written form to IT department

8. **Exempted sites blocked again.** Internet sites change on a daily basis and your sites' path may have changed - or they may have changed providers for their home page. The County downloads a control file daily that has all the latest sites and their paths. If your site has changed, and when you download this file it could become blocked again. If this is the case, please contact us.

9. **Department Leaders** are encouraged to review current and future possibilities of Internet access by their departments and to provide a memorandum to the CTO listing any resources available on the Internet or uses that department could make of the Internet. Recommendations for Internet access and usage, including service providers and cost estimates, should be included in the memorandum.

10. **Access restricted by proxy server.** All *browser* access to the Internet for World Wide Web and FTP (file transfer) is required, by policy, to pass through a "proxy" server that has been installed for this purpose. Browsers not configured to use the proxy server will not be allowed direct access to the Internet.

Be advised that Smith County now employs software that will monitor all sites visited by every computer on the County Network. A list will be furnished to each Department Head on a routine basis, listing all sites visited by their associates.

Violation of any part of the Smith County Information Technology Policy can result in denial of access to parts of or all systems within the County Network. Associates and supervisor(s) will be notified of any violations prior to corrective action(s). The IT Department has discretion to eliminate access to sites on the Smith County Network.

PENAL CODE

Penal Codes, Chapter 33 "Computer Crimes". Section 33.02 (B) states the following:

(A.) A person commits an offense if the person knowingly accesses a computer, computer network, or computer system without the effective consent of the owner.

(B.) A person commits an offense if the person intentionally or knowingly gives password, identifying code, personal identification number, debit *card* number, bank *account* number *or* other confidential information about a computer security system to another person without the effective consent of the person employing the computer security system to restrict access to a computer, computer network, computer system or data.

(C.) An offense under this section is a Class A misdemeanor unless the actor's intent is to obtain a benefit or defraud or harm another. In which event the offense is:

1.) A state jail felony if the value of the benefit or the amount of the loss or harm is less than $20,000; or
2.) A felony of the third degree if the value of the benefit or the amount of the loss or harm is $20,000 or more.

(D.) A person who is subject to prosecution under this section and any other section of this code may be prosecuted under either or both section.