SECTION 28
COMPUTERS, INTERNET AND ELECTRONIC COMMUNICATIONS

A. GENERAL:

1. Any county department eligible for and having funding for the Internet will be provided with access under the terms and conditions of this policy. Violation of this policy may be grounds for having access to Internet or other electronic communications services revoked.

2. The objective of this policy is to minimize the risks to business functions and government-owned assets, and to assure adherence to regulatory and legal requirements and enterprise policies when county resources are used to access public networks.

3. The scope of this policy applies to electronic communications on public networks such as:

   a. electronic mail;

   b. file transfer;

   c. remote login;

   d. remote control software;

   e. discussion groups;

   f. World Wide Web, Gopher, Web Servers, Wide Area Information Servers;

   g. Internet;

   h. America Online, CompuServe, Prodigy and similar services;

   i. online search services such as Dialog or Paperchase; and

   j. dial-up bulletin board systems.

B. PRIVACY CLAUSE:

1. The contents of an employee's computers and electronic mail are subject to search without the employee's consent. An employee shall have no expectation of privacy to electronic communications sent or received by that employee. Electronic media, specifically the Internet and e-mail, is not a secure communication network and personal or privileged information sent via these media could potentially be read or disclosed by anyone.

2. The county may access, monitor and disclose the contents of employee electronic messages, Internet contacts and communications, and other information received or transmitted by electronic media. Circumstances in which access, monitoring, and disclosure will occur may include, but are not limited to:

   a. suspected misuse of electronic media;

   b. investigation related to pending or anticipated litigation;

   c. ensuring compliance with this policy, applicable laws, ordinances, or court orders;

   d. ensuring appropriate use for county business; and

   e. accessing information in the employee's computer system when the employee is unavailable.

C. **INTERNET ISSUES**: Internet access can provide significant business benefits for county government. However, there are also significant legal, security, and productivity issues related to how the Internet is used. Examples of such issues are the potential:

   1. to receive computer viruses from Internet information sources;

   2. for someone to eavesdrop on data or correspondence which is exchanged via the Internet;

   3. for a county employee, through the content of their Internet exchanges, to impugn the reputation of local government officials and thereby invite civil liabilities;

   4. for county employees to be enticed by the vast social and informational forums of the Internet into spending significant work time on nonproductive activities;

   5. of county employees or any person using an Internet connection to sufficiently upset other Internet users, causing the connection to be flooded with traffic in protest, thus negatively impacting the availability of the service for true business purposes; and

   6. for outside access to local databases to overwhelm the processing power of the local network.

D. **GUIDELINES**: The following procedures shall be followed while accessing public networks through county resources. These guidelines govern both county employees, contractors, and anyone working under county direction.

   1. Use of county resources for accessing public networks is for work related purposes only.

   2. Act responsibly when participating in discussions over a public network. Be polite and do not get abusive in your messages to others. Defamation can occur due to malicious use of the Internet.

3. Do not use public networks inappropriately. Use may be monitored and access may be revoked at any time for inappropriate conduct.

4. Determine and abide by the policies and procedures of any external network you access. You are expected to be a "responsible network citizen".

5. Downloading of any software programs or applications including shareware, freeware and demo's is strictly prohibited. All such requests must go through Information Services.

6. When downloading non-application software, check for copyright or licensing agreements. If there is any doubt, do not copy. If a licensing agreement exists or you must pay for the information, it must first be approved by the Information Services Data Board.

7. There should be no automatic requests for information on the Internet.

8. Avoid the generation of excessive electronic mail.

9. The target directory must be scanned with anti-virus software before and after downloading any files from the Internet. As most downloads are in a "zipped" format, scanning the files after "unzipping" is necessary. It is the user's responsibility to insure that the downloaded files are free from known viruses.

10. Do not use software which attempts to discover properties about the public network or computing resources connected to that network.

11. Any data transferred via the Internet is prone to be monitored and intercepted by unintended destinations.

12. All electronic mail is a public record and may be subject to public inspection.

E. ROLES AND RESPONSIBILITIES:

1. Information Services shall:

   a. provide updates and suggestions for this policy;

   b. apprise elected officials and department heads of any continued abuse;

   c. not act as the "Net Police";

   d. not be held responsible for non-professional usage, improper humor, or the moderation and monitoring of electronic mail or Usenet groups. Disciplinary actions for sexual harassment and hostile work environment violations and for use of county property for personal purposes are defined by other county policies.

2. The Information Services Data Board shall:

    a. review and approve the Internet Acceptable Use Guidelines; and

    b. advocate adherence to the policy.

3. County departments shall:

    a. act as the authorizing agent that allows access to the Internet;

    b. ensure that the acceptable use guidelines are followed;

    c. provide for training of employees who need access;

    d. budget for service and associated training, if needed; and

    e. establish their own data sensitivity policy.

F. PROTECTING PROPRIETARY INFORMATION:

1. Persons transmitting enterprise data over public networks should ensure that the data is processed according to its level of sensitivity by using the definitions and guidelines which follow. After having read the following sections, if you are unsure of how to properly handle specific data, contact the data custodian for guidance.

2. Data Sensitivity Definitions:

    a. "Confidential Data" means information that shows specific strategies and major directions; information so defined by local, state or federal laws, rules or regulations; or data of other business or persons with respect to which the county is under an obligation of confidentiality.

    b. "Protected Data" means working files not completed for public dissemination; data which is of such a nature that unauthorized disclosure would be against the best interest of the county; or is personnel data with restricted use or access per local, state or federal laws, rules or regulations such as criminal justice data.

    c. "Private Data" means all county-related information requiring baseline security protection but failing to meet specified criteria for higher classifications including organizational policies and procedures that are internal by nature, and internal announcements.

    d. "Public Data" means information which requires no security protection such as public information, public announcements, and internal correspondence and documentation which do not merit a security classification.

3. Data Sensitivity Processing Guidelines:

Confidential	Protected	Private	Public
Encrypted	Encrypted	Owner defines permissions	High Volume Use other alternatives (mail carrier)
Owner defines permissions	Owner defines permissions	High Volume Use other alternatives (mail carrier)	
Marked confidential	High Volume Use other alternatives (mail carrier)		
Electronic confirmation required			
High Volume Use other alternatives			

G. <u>SECURITY</u>: There are hundreds of millions of pages of Internet information and billions of publicly available files. It is impossible to monitor every site in the world to determine if the site has material available which violates policy. Even if a specific item is in violation of county standards, blocking access will not prevent access to the material, as many sites are either mirrored at other locations, or change their name and Internet protocol number regularly to avoid prosecution.

H. <u>MODEM SECURITY</u>: The following modem security guidelines shall be adhered to:

1. When utilizing a modem for remote access to another computer, the employee must be aware of and follow the acceptable use policy, if any, regarding the remote system.

2. There is no such thing as a 100 percent secure system. The human element is always the weakest link in system security.

3. Passwords must be secure. Do not share passwords or write passwords on paper. It is recommended that a password consists of letters and numbers.

4. Within the software which controls the modem, the "answer off" mechanism shall be exercised in all situations, unless otherwise approved by Information Services.

5. If one elects to download non-application software, the download directory must be scanned with an anti-virus program immediately following the download. Information Services will train the end-user on utilizing the anti-virus program. If you have a modem and are on the county network, it is possible for a virus to attack any or all networked computers.

6. Do not distribute the phone number of the shared or dedicated modem line unless it is absolutely required.

7. If the phone number to the remote system is long-distance, keep the call to a minimum length as possible.

8. If the modem is external, turn it off when the modem is not in use.

I. INTERNET ACCEPTABLE USE GUIDELINES:

1. This subsection represents a guide to the acceptable use of the Internet for county employees. This subsection intends only to address the issue of Internet use. In cases where data communications are carried across other regional networks, acceptable use policies of those other networks apply and may limit use.

2. Participating agencies assume the responsibility for providing reasonable publicity and enforcement for this policy. Ultimate responsibility for traffic that does not conform to this policy lies with the individual end user. Each county department shall monitor and rectify the behavior of its users who disregard this policy.

3. Departments shall provide adequate training for their users to ensure appropriate network use.

4. Information Services and the county accepts no responsibility for the traffic which it transports and which violates the acceptable use policy of any connected networks, beyond informing the county department if and when a violation is brought to the attention of the Data Board.

5. All use of the Internet must be consistent with the goals and purposes of the Internet and within the spirit of this policy. The guidelines listed herein are provided to make clear the categories of use which are consistent with the purposes of the Internet. The intent is not to exhaustively enumerate all such possible uses or misuses.

6. Internet computing resources are world-wide, and all users are urged to exercise common sense and decency with regard to these shared resources. Particular attention should be paid to policies developed for various Internet services by Internet users, such as Usenet policies.

7. Because of the diversity of resources on the Internet, an even moderately complete listing of do's and don'ts would be quite large. In general, common sense should be used to judge situations. The following guidelines are given as a starting point.

   a. Computing resources should be used only in the support of the administrative, instructional, and research objectives of the county.

   b. Appropriate use of resources is limited to the official work of the departments.

c. Examples of inappropriate use of resources include:

    (1) any traffic that violates state, local or federal laws;

    (2) any traffic that is unethical in nature;

    (3) distribution of unsolicited advertising;

    (4) propagation of computer worms or viruses;

    (5) distribution of chain letters;

    (6) attempts to make unauthorized entry to another network node;

    (7) use for recreational games;

    (8) personal use; or

    (9) sexually offensive material.

d. Respect the privacy of others. Do not seek information about, obtain copies of, or modify electronic information belonging to other users unless explicitly authorized to do so by those users.

e. Do not share passwords with others or use passwords not belonging to you.

f. Respect appropriate laws and copyrights. The distribution of programs, databases, and other electronic information resources is controlled by the laws of copyright, licensing agreements, and trade secret laws. These should be observed.

8. All departments must follow these guidelines and understand that network traffic originating from their location is to be consistent with this policy. Information Services cannot police the network but may refer to the appropriate office holder for disciplinary action any department or employee that appears to be in persistent or serious abuse of this policy. Questions pertaining to the policy or interpretation of the policy should be submitted to the Data Board.

9. Information Services may at any time make a determination that particular uses are not consistent with the purposes of the Internet connection. Such determinations will be reported to the department head, as appropriate, for information and possible imposition of sanctions. Persistent or serious violations of the policy may result in withdrawal of approval to use the Internet or other penalties.

J. PARTICIPATION IN DISCUSSION GROUPS:

1. There should be a good business reason for participating in any discussion group over the Internet.

2. Even in a discussion but not limited to a discussion, the user must be aware that the information he or she puts out on the Internet will be perceived as the official Tooele County position unless specifically identified as personal opinion. If you are offering your own opinion, be sure it is clearly identified as such. Also, a good rule of thumb is: "If you would be embarrassed to have someone read it on a postcard, don't say it on the Internet."

3. All the rules which apply to other forms of written correspondence apply here, even though the style is more casual.

K. CLASSES OF MAIL ALLOWED: Setting the standards for both casual and official correspondence is the responsibility of the individual department and would be the same for the Internet as for other forms of written correspondence.

L. QUALIFICATIONS FOR ACCESS AUTHORITY: Before Information Services approves a user for Internet access, a Tooele County Computer Security Request Form must be properly filled out and according to the normal procurement process.

M. WEB SERVER GUIDELINES:

1. Information Services and the Tooele County Data Board will review all Web access proposals to ensure the project adheres to all guidelines set forth in this section. Any proposed Web access must be submitted to the Information Services Data Board for initial approval of the proposed project.

2. The following information must be provided to Information Services for them to review and assist in submitting the initial request to the Data Board:

   a. the project's general purpose and how it relates to Tooele County business;

   b. the scope of the project, including what information is going to be made available and to whom and who is the targeted user of the project;

   c. initial design documentation, which includes a rough page layout, applets, links, images, etc.;

   d. identification of Tooele County data accessed that is not located on the web server and indicate how the data will be used;

   e. the designated contact person within the department for this project and who will be responsible for maintaining current information; and

   f. the security requirements of the project.

3. If initial approval is granted for the project, the following guidelines shall be followed during the development:

a. Information Services must establish and maintain a fully functioning firewall for web access projects to be operating in production.

b. Information Services will monitor applications and network activity and set restrictions as needed to prevent problems with Tooele County data or internal network processing.

c. Appropriate security levels will be maintained by Information Services.

d. Information Services will approve and allocate resource requirements.

e. To help ensure compatibility between applications, development tools as defined by Information Services and approved by the Data Board will be used.

f. Information Services must first review and approve the proposed location of the data and Web page access, Web server, and network access points.

g. All development or enhancements to a project must be performed and tested on a designated test Web server.

h. After testing is completed and the project is reviewed by Information Services, the project will be transferred to the production Web server. Only Information Services will have development access on the production Web Server.

i. Information Services' main priority is to maintain the integrity of the Tooele County data and in-house network processing capabilities. If at any time, the web page or associated links or controls do not adhere to the set standards or cause a problem for whatever reason, the web page may be terminated without notification.

j. Contents of web pages should be approved by the department head or elected official or his or her designee.

N. USE OF ELECTRONIC MAIL:

1. Electronic mail ("e-mail") is any message that is transmitted electronically between two or more computers or terminals, whether stored digitally or converted to hard copy. All computer-related information, including e-mail messages, are the property of Tooele County and are considered the county's records.

2. All county employees with a need will be assigned a user's address by Information Services. These addresses may be used to send and receive e-mail messages to and from other county employees.

3. Elected officials and department heads may request an e-mail address that is Internet-accessible. At the request of the department head or elected official, employees will be provided Internet-accessible e-mail addresses for conducting county business. Employees will be provided such e-mail addresses, pending county technology capabilities and availability. Continued access to Internet-accessible e-mail will be contingent upon the employee's conduct. Costs associated with e-mail access will be evaluated annually and determined through the County's budget process.

4. As with any county property or equipment, e-mail should be used for official county business only. However, strictly forbidden e-mail usage includes use for personal profit or gain; transmission of political messages; solicitation of funds for political or other purposes; or sending of harassing messages.

5. Because e-mail is county property, the county has the right to inspect and review any e-mail or other data stored on county computers or equipment. Information Services is responsible for monitoring electronic mail through regular computer and network maintenance. Additionally, county officials may inspect and copy e-mail and computer records when there are indications of impropriety by an employee, when substantive information must be located and no other means are readily available, or when necessary for conducting county business. Supervisors may review the contents of an employee's electronic mail without the employee's consent.

6. E-mail messages that concern policies, decision-making, specific case files, contracts or other information that should be kept as part of the official records of county business should be retained by the recipients of such e-mail. Therefore, employees are responsible for retaining and archiving electronic mail messages as official records of county business. E-mail messages should be stored on the county's network drives.

7. The director of Information Services is the official custodian of electronically and digitally stored information, including electronic mail. Information Services is responsible for monitoring and retrieving archived data.

8. Employees are responsible for archiving e-mail messages. After 45 days, employees should delete e-mail messages to minimize storage requirements. Information Services is responsible for long-term storage of e-mail and will retain and destroy e-mail records in accordance with the records retention schedules established for records by the State.

9. Public requests for electronic mail that is a public record should be submitted to the elected official or department head. Requests for public records will be handled in compliance with the Government Records Access and Management Act. If a request is made to inspect e-mail, county staff shall prior to release consult with the elected official or department head for the purpose of determining whether the correspondence is a public record. Members of the public who request public e-mail records will be charged for the costs of providing those records, in accordance with the county fee schedule.