COUNTY OF ORANGE, VIRGINIA
PERSONNEL POLICIES MANUAL

USE OF COMMUNICATIONS EQUIPMENT AND TECHNOLOGY

POLICY NO.: 3.11 **EFFECTIVE:** 3/14/00
REVISED: 11/12/2003

OVERVIEW: This policy defines the parameters of employee use of County communications equipment and technology such as voice mail, e-mail, external electronic bulletin boards, online services, intranet, Internet and the World Wide Web.

SCOPE: This policy applies to all County employees regardless of employment status.

DEFINITIONS:

Communications Equipment – computer hardware and software, pagers, cameras, laptops, tablets, personal digital assistants (PDA), cellular phones, phone systems, copiers, scanners, fax machines, and wireless systems.

Data – Information which is processed, stored, maintained, or transmitted on computing systems and networks. This includes: email, County documents, memorandums, letters, etc.

Hacking- Attemping to enter a system when a password has been lost or forgotten, debugging a copyright software program, or testing a system's security or network.

Pinging – To test whether a particular network destination on the Internet is online by bouncing a "signal" off a specified IP destination address.

PROVISIONS:

A. <u>General Use of County Communications Equipment and Technology</u>

Communications equipment purchased, leased or rented by the County is the property of the County and is to be used primarily for County purposes. In some cases, communications equipment may be assigned to one employee or shared by a group of employees.

County communications equipment and technology may not be used to solicit others for commercial ventures, religious or political causes, outside organizations, or other non-business matters. The use of County communications equipment and technology to engage in an illegal act is strictly prohibited.

Generally, electronic information created and/or communicated by an employee using County communications, equipment and technology is not reviewed by the County. However, the following conditions should be noted:

The County routinely gathers logs for most communications and electronic activities for the following purposes:

1. Cost analysis;

2. Resource allocation;

3. Optimum technical management of information resources; and

4. Detecting patterns of use that indicate employees are violating County policies or engaging in illegal activity.

The County reserves the right, at its discretion, to review any employee's electronic files and messages to the extent necessary to ensure electronic media and services are being used in compliance with the law, this policy and other County policies.

Employees should not assume electronic communications are private. Accordingly, if they have sensitive information to transmit, they should use other means.

B. <u>Use of E-mail Services</u>

At times, County employees send and receive "personal" email on County computers, just as they occasionally make and receive "personal" phone calls on County phones. Like personal phone calls, the receiving and answering of personal e-mail should be kept to a minimum, and, when possible done outside of normal work hours.

Most e-mail messages and other contents of the hard drive, floppy/zip disks or CD/DVDs, on County computers are subject to the Virginia Public Records Act. To the extent such messages have been preserved, they are subject to public disclosure under the Freedom of Information Act (FOIA) unless a specific exception to the mandatory disclosure requirement exists. E-mail and other electronic records on County computers must also be produced if subpoenaed. In this regard, e-mail records are no different than any other letter, memorandum, or other document generated in the conduct of
public business.

Electronic correspondences should be treated as something that could conceivably end up on the front page of the local paper and therefore:

1) All unimportant e-mail (i.e. not important enough to keep as a matter of official record) should be treated as routine and deleted.

2) At least every 30 days, County employees should empty the "trash" folder on their computer browser to permanently remove email from the hard drive.

Electronic media cannot be used for knowingly transmitting, retrieving, or storing any communication that is:

1. Discriminatory or harassing;

2. Derogatory to any individual or group;

3. Obscene, sexually explicit or pornographic;

4. Defamatory or threatening;

5. In violation of any license governing the use of software; or

6. Engaged in for any purpose that is illegal or contrary to this policy or business interests.

7. Attempting to hide the identity of the sender or represent the sender as someone else.

C. <u>Computer Software</u>

Orange County purchases and licenses the use of various computer software for business purposes and does not own the copyright to this software or its related documentation. Unless authorized by the software developer, the County does not have the right to reproduce such software for use on more than one computer. The County does not permit the loading and use of any software on County equipment without the written approval (a work order), authorization, or installation assistance from County Information Technology (IT) Staff. County employees may only use software on local area networks or on multiple machines according to the software licensing agreement. The County prohibits the illegal duplication of software and its related documentation.

D. <u>Encryption</u>

Employees can use encryption software supplied to them by the IT Staff for purposes of safeguarding sensitive or confidential business information. Employees who use encryption on files stored on a County computer must provide their supervisor with a sealed hard copy record (to be retained in a secure location) of all of the passwords and/or encryption keys necessary to access the files. The supervisor must also provide a copy to the IT Staff.

E. <u>Security</u>

No person may utilize the County communications equipment and technology except to the extent specifically authorized. Employees should not access files, load software, retrieve any stored communication, or destroy County records (worksheets, spreadsheets, County memos/letters) without authorization. Assisting or encouraging others to take any action that would result in unauthorized access, transmission, duplication, loss or modification of data or records is prohibited.

The IT Staff is responsible for creating user-IDs with the associated access privileges granted by the appropriate Department Director or Constitutional Officer, for maintaining an appropriate level of overall system security, and for monitoring the system for security violations. IT Staff shall also maintain records for all accounts including appropriate signatures and access privileges granted. Such records shall be maintained for two years after account termination.

Only those employees with operational requirements will be granted access to systems. Access privileges are determined by a person's job duties. Access is granted by means of a computer account which has an associated user-ID.

Access to computer accounts must be protected, at minimum, by a user-ID and password. It is the responsibility of the user to safeguard his/her user-ID and password. A user-ID is not to be shared; the password is not to be divulged to others.

- A user-ID and password are required to access any system.
- A user-ID must be at least six characters long.
- Passwords must be at least six characters long. Restrictions on password complexity are system dependent.
- Passwords must be changed at least once every 90 days.

When a user no longer works for the County or assumes different job duties within the County, it is the responsibility of their supervisor to request that his/her user-ID be deleted no later than the date of termination or transfer. If a transferred employee needs access in a new job, a new user-ID must be obtained. User-IDs will be terminated if they are inactive for a 90 day period.

Access to computer accounts may be suspended at any time if security violations or misuse are suspected. A user-ID will be suspended when an incorrect password is entered five consecutive times.

Procurement of Communications Equipment

All procurement of communications equipment will be processed by IT Staff and will be assigned to the appropriate department through this acquisition process. Each department is accountable for that equipment until removed by IT Staff.

Individual Responsibilities

Individual employees are responsible for maintaining the security and confidentiality of data in their possession or on their workstations. Computers need to be password/screen saver protected when away from the desk. Individuals must report to the appropriate security administrator any known breach of application or system security. Individuals who have constructive suggestions to improve security are encouraged to propose them. Individuals are responsible for shutting down computers at the end of the day. Individuals are required to backup all documents on the network server. If a server is not available, all backups are required via disk, cd or dvd. IT Staff is responsible for backing up servers each night.

Training and Testing

IT Staff shall provide user training on security issues when new Systems are installed.

Guidelines for Electronic Communications

Employees must respect the confidentiality of other individuals' electronic communications. Except in cases in which explicit authorization has been granted by the IT Staff, employees are prohibited from engaging in, or attempting to engage in:

1. Monitoring or intercepting the files or electronic communications of other employees or third parties (Supervisors are authorized to monitor); and

2. Hacking or obtaining access to systems or accounts they are not authorized to use. This is to include pinging or attempting to hack IP addresses and firewall; and

3. Using other people's log-ins or passwords on server and AS400; and

4. Breaching, testing, or monitoring computer or network security measures. and

5. Using personal equipment such as laptops, etc. to connect to the County network.

Electronic media and services should not be used in a manner that is likely to cause network congestion such as downloading video streaming, downloading MP3's, playing internet games or significantly hamper the ability of other people to access and use the system.

Anyone obtaining electronic assess to other companies' or individuals' materials must respect all copyrights and cannot copy, retrieve, modify or forward copyrighted materials except as permitted by the copyright owner.

Employees should notify their immediate supervisors, technology staff, or the County Administrator upon learning of violations of any of these policies. Employees who violate these policies will be subject to disciplinary action, up to and including termination of employment.