POLICY AND PROCEDURES

NUMBER: 133 **SUBJECT: Electronic Communications**

ACA STANDARDS: None

DIRECTOR: Herbert Bernsen

EFFECTIVE DATE: 10/98 **REVISION DATE: 5/01, 8/03, 1/08, 4/09, 10/12, 11/14**

:

I. POLICY

The St. Louis County Department of Justice Services will establish guidelines as to the proper use of the electronic communications systems.

II. RESPONSIBILITIES

All St. Louis County Department of Justice Services' staff are responsible for the following procedures.

III. DEFINITIONS

Spyware: software that reveals identity of user: software surreptitiously installed on a hard disk without the user's knowledge that relays encoded information on his or her identity and Internet use via an Internet connection.

IV. PROCEDURES

A. To support its operations, the St. Louis County Department of Justice Services provides electronic communication tools, such as, phones, cellular phones, computers, facsimile (fax) machines, etc. These resources are to be used for business purposes only and no personal use during working hours is intended or approved.

B. There are additional guidelines for the proper use of electronic communications in the County Information Technology Policies (02.00 E-mail Use and Management and 03.00 Internet/Intranet/WWW and Web Site Use and Management).

C. Users of the Internet will comply with the following usage limitations:

1. Employees will have authorization from the Director of the Department of Justice Services to have access to the internet on their computers, except for use in the Computer Lab. No Department Head shall authorize access to the County intranet for non-County intranet users without the approval of the CIO.

2. The County retains all rights to any material posted to any forum, newsgroup, chat or WWW page by any employee or person, covered in the Scope section (See County Policy 03.00 Information Technology (IT) Policies) in the course of his/her duties.

3. Do not download games, chain letters or anything that will be stored on the hard drive

4. Do not use any unauthorized programs on the Department of Justice Services' system that may circumvent the security system

Note: The purposeful installation of spyware on county computers is prohibited.

5. Accessing web sites containing inappropriate content including, but not limited to:

a. sexually oriented and/or explicit material and/or anything that would violate St. Louis county's policy against gender discrimination and harassment

b. Hate-oriented material

Downloading contents from these sites and/or sharing this content is prohibited.

6. The downloading and sharing of inappropriate content from the internet is strictly prohibited and is subject to disciplinary action.

7. Staff members are responsible for all software and files that they place on the Department of Justice Services' system

8. Users shall not use social networking sites (e.g., Facebook, Twitter, My Space) for County business without prior approval of their Department Head and the Chief Information Officer.

NOTE: Employees shall not post County information on social networking sites without the prior approval of their Department Head.

9. Staff members will ensure that all Department of Justice Services' data is properly safeguarded according to its nature.

[D. E-mail *and instant messaging* will be used in the legal and appropriate sharing of information to support and enhance the County's business. Individual departments will determine who administers the policy for use in their department, including e-mail access and appropriate disciplinary action(s).]

E. Staff members will not save or forward any e-mail (pictures, cartoons, jokes, material of a sexual nature, etc.) that is not to be used for business purposes. All unwanted or unsolicited e-mails that are not business related will be deleted and the trash emptied immediately. If there are any concerns regarding the e-mail system the staff member will direct questions to his/her supervisor and/or Division Manager.

F. Electronic harassment of any kind the use of threatening, insulting, obscene and abusive language, the use of derogatory remarks based on religion, race, color, sex, disability or national origin or remarks that are defamatory toward any person is prohibited.

G. Section Redacted. Portions of this record are closed pursuant to Section 610.021(19) RSMo and Section 114.020(18) SLCRO because public disclosure of such portions would threaten public safety by compromising the safe and secure operation of the Jail, and the public interest in nondisclosure outweighs the public interest in disclosure of the portions of such records.

H. Unauthorized access to the e-mail account of another is prohibited. Only Department Directors/designees (Department Heads) and the REJIS E-Mail System Administrator have authority access to e-mail accounts.

I. Only the County's e-mail system can be used to conduct County business. The use of non-County e-mail systems to conduct County business is prohibited.

J. E-mails messages take up disk space, and the computer on which you reside may have quotas on disk space. It is best not to save every message you receive. In any case, you should adhere to the St. Louis County document retention policies (See County Policy 02.00 E-mail Use).

K. All equipment owned by the Department of Justice Services is to be used for approved purposes only. Appropriate action will be taken for the unauthorized or improper use of the electronic communication systems which include sending or accessing offensive or inappropriate materials, as well as unrelated work material. General Broadcast messages to multiple users in the Outlook Address Book will be performed for business purposes only and by the direction of the Director/designee. Any questions regarding appropriate use of communications equipment will be referred to the staff member's supervisor.

L. Software in use by a Justice Services staff member on his/her computer work station will be properly licensed. Audits will be conducted periodically to ensure compliance to these procedures.

M. If a staff member has existing software on a computer workstation that is not properly licensed it will be removed. Unlicensed software discovered during an audit will be immediately deleted with possible disciplinary action taken. All software license restrictions and copyrights will be honored.

NOTE: The criminal penalty for illegal sharing of software is expensive and the staff member will be held liable.

N. The introduction of any personal software (e.g., screen savers, desktop photos, icons, etc.) without the approval from the Superintendent of Security/designee is prohibited.

O. Staff are not allowed to load games into the computer at work or play computer games (e.g., solitaire, mine sweep, etc.)

P. Staff attempting to purchase computer-related equipment, supplies or resource material or attend a computer training class for work will be required to have a recommendation from the appropriate Superintendent of Security/designee for approval.

Q. Staff will at no time make changes to or remove any information related to the base programs of the computer system. This includes making changes to the appearance of the desktop, adding or deleting icons, changing color schemes, or changing wallpaper. This may cause damage to the operating system and make the computer unusable.

R. St. Louis County IT Policies will also be adhered to concerning computers. County IT Policies may be accessed using the intranet.

S. Report the malfunction of or any changes to the following electronic communications equipment to the proper authority:

1. Computers – REJIS Helpdesk (314-535-9497)

2. Cellular Phones – Superintendent of Security

[3. Staff Telephones – *Security Electronics Administrator]*

4. Facsimile Machines – Appropriate Office Supervisor

T. If an employee becomes aware of any violation of this policy, it is that staff member's responsibility to immediately report the violation to his/her supervisor, Division Manager or the Superintendent of Security/designee. When a supervisor becomes aware of an electronic communications violation, he/she will report the violation to the Director, Superintendent of Security/designee.

U. Refusing to cooperate with a security or policy violation can result in disciplinary action.

V. Wireless Communications

1. Personal calls are not permitted on County issued equipment, unless the employee chooses to purchase an alternative service plan.

NOTE: Per Policy 809 Use of Mobile Phones, Staff assigned with a mobile phone may use the mobile phone for family emergencies or to inform family members that he/she will be working later than expected. Staff are responsible for the cost of any personal phone call.

2. The employee is responsible for the care and custody of the equipment and any or all damages, including theft, which occurs through negligence or neglect. Such damage or loss will result in reimbursement by the employee to the Department.

3. It is the employee's responsibility to return all equipment in good operating condition to the Department upon resignation or termination.

4. Supervisors will review and validate usage statements.