

# LSSCM Technology Policies

Updated October, 2006

[Bob Gillett](#) and [Steve Gray](#)

## I. VOICEMAIL AND E-MAIL

Staff are responsible for checking and responding to voicemail and e-mail messages regularly. In general, communications through either of these systems should be checked at least daily. If you're not going to receive voicemail messages for longer than three days, you should leave a message to that effect on your voicemail. Voicemail and e-mail communications should be acknowledged and responded to as any other written communication or phone message.

Staff should not make any communication using the voicemail or e-mail system that shouldn't be made in a letter or memorandum. Each of these systems presents its own opportunities for humor. However, sometimes things that seem funny at the time appear cruel or otherwise objectionable when received in an e-mail or a voicemail message. Please be aware of this and try to avoid humor that may cause hurt feelings.

E-mail is confidential. You should not read other people's e-mail without their permission.

## II. USE OF THE INTERNET

The program's connection to the Internet exists to assist us in our legal work-- contacts with funders, research, e-mail, etc. Except as provided in Section IV of this policy, all Internet shall be work-related.

Please keep in mind that Internet use is traceable. No staff person should use program equipment for purposes prohibited by program policies or that could not be reasonably explained to persons outside the program.

## III. OWNERSHIP OF PROGRAM EQUIPMENT AND TECHNOLOGY

### **A. All equipment and technology is owned by LSSCM and subject to monitoring by management.**

All computers, computer software, telephone systems, fax machines, copier machines, voicemail systems, e-mail systems, and Internet access systems within the LSSCM offices are the sole property of LSSCM. In order to assure that the primary use of these systems is the provision of legal services to the poor in compliance with program policies, program priorities, and program grant requirements, LSSCM has the right to monitor and control the use of all its property, equipment, and systems. No individual staff member has any proprietary or confidential interest in any materials stored or copied in any office files or systems, including voicemail and e-mail. Any material in any LSSCM system may be monitored, copied, or purged by the program management at any time.

### **B. Seek permission before installing software on your computer.**

Currently LSSCM does not "lock-down" desktop computers to prevent software from being installed by individual users. However, users must get permission from both their managing attorney and the program wide CRP before installing additional software on their computer. In the past we have found that some users have installed non-work related software that opened up their computer to virus attacks and generally degraded system performance. We would like to avoid this in the future without compromising staff's ability for meaningful computer use.

## IV. PERSONAL USE OF PROGRAM EQUIPMENT AND TECHNOLOGY

Employees are permitted reasonable personal use of program equipment provided that: (a) this use occurs on that staff person's personal time; (b) the staff person reimburses the program for any direct costs associated with the use; (c) this use doesn't interfere or conflict with LSSCM's programmatic use of the property, equipment, or system.

## V. DATA STORAGE

### A. All staff should place case-related computer documents they work with in the appropriate common directories.

LSSCM currently utilizes local area networks (LANs) in each office. Under our system, portions of server hard drives have been set aside for access from every computer on the office LAN. To take advantage of this information sharing capability several root directories have been created on servers in each office and organized for common storage of office computer files.

The most important of these common root directories is the **Document Share**, typically labeled G:\ in most offices (or H:\ or I:\ in others). Every office has a Document Share directory that is accessible to every computer on the LAN. This is where case related and other work-related documents should be stored. The Document Share is organized by case-handler. Each Document Share has a separate sub-directory for every casehandler in that office. Documents generated for or by a particular casehandler should be placed in that casehandler's sub-directory. For example: The Washtenaw office has a sub-directory of G:\ called G:\PS\. This is Paul Sher's sub-directory. All documents generated for or by Paul should be saved to G:\PS.

### B. Use of Sub-Directories

If you anticipate that a case or a project will generate 10 or more documents (or if a case has generated numerous documents and you want them organized better) you should create a sub-directory to store all the documents from that case or project.

One such sub-directory has already been created in each casehandler's directory called "CL". You should use the "CL" sub-directory for storage of case-related materials. For example, all case related documents generated for or by Ann Routt should be placed in G:\AROUTT\CL.

## VI. CLEANING UP YOUR DIRECTORIES

Over time, your directories will become full and this may make locating documents more time consuming. We suggest that you periodically (at least once a year) clean out your directories. This can be done by deleting files that are no longer relevant. It is probably a better practice to create a sub-directory for non-current materials-- e.g., G:\PS\OLD\. Any non-current documents (e.g., files relating to closed cases) can be moved to this sub-directory where they will be "out of the way", but can be retrieved in the future if they are needed for any reason.

## VII. CONFIDENTIALITY

### A. Common Files and Confidential Documents

There are times when we need to keep a word-processed document confidential. Confidential documents should not be stored on the Document Share (i.e. G:\).

Managers have private directories on the network for storing confidential documents. These directories are password protected and should not be accessed by staff without a manager's

permission.

Other confidential documents can be stored on your local hard drive (C:\) or removable storage media (flash/thumb drive or CD). If you have a document you want to be confidential both Word and Windows allows users to create password protected documents. If you have questions about how to do this, talk to your office CRP. You can either store a confidential document on your local hard drive then password protect it or store it to a removable storage media.

#### **B. E-Mail**

E-mail is confidential.

You should not read other people's e-mail without their permission.

### **VIII. COMMON AREA CONSIDERATIONS**

#### **A. File Protection**

When working in common directories you should never delete a file unless it was created by or for you—and even then use caution. Before you modify a document not created by or for you copy it to a new file name in your directory.

#### **B. Use of the E-Mail System.**

Staff should not make any communication using the e-mail system that shouldn't be made in a letter or memorandum.

### **IX. OPEN SOURCE SOFTWARE**

LSSCM supports the use and creation of open source software as generally in line with our values as a nonprofit poverty law program. We will endeavor to use, support and contribute to open source software in our program whenever feasible.