

Office Sharing Tips

By Susan Traylor, Practice Management Advisor
Law Office Management Assistance Program

What is office sharing in the context of law firms? Two or more law firms, operating as independent law firms, but sharing one or more of the benefits and overhead expenses related to the operation of their firms.

Benefits of sharing office space with another attorney or business.

- Reception
- Photocopies
- Mail service/Postage
- Library
- Conference room
- Runner/Courier service
- Phone system
- Facsimile
- Computer technical support
- Décor
- Camaraderie
- Building Security
- Built-in referral source
- Amenities of a larger office building, i.e. gym, restaurant, parking

Issues to Consider when sharing office space with another attorney or business

- Advertising: How do you hold yourself out to the public?
- Conflicts of interest
- Client confidences
- Compatibility with suite-mates
- Reputation of suite-mates

➤ **Advertising (how you hold yourself out to the public)**

- Names on Door: Should appropriately reflect individual firms
- Business cards: Should appropriately reflect individual firm
- Letterhead: Should appropriately reflect individual firm
- Fee agreement: Should appropriately reflect individual firm

Malpractice insurance carriers often recommend specific terminology in fee agreement clarifying the distinction between your firm and the firm(s) with which you share office space. For example:

“The Client acknowledges that _____ has an office sharing arrangement with _____. Client acknowledges that no attorney relationship exists between he and _____”

Confidentiality of Client Information

➤ **Staff-Sharing**

Sharing a receptionist, secretaries, paralegals and/or other support staff requires careful consideration. Typically, sharing a common receptionist whose responsibilities are merely to direct incoming calls and greet clients and other visitors, is not a problem so long as no confidential information is passed on to the receptionist during the process. However, as the duties of the shared receptionist expand to include more detailed processing, i.e. determining which attorney in the suite to whom to direct the client based on practice area, questions may arise, in particular with regard to ethical rules on group advertising and referral services.

➤ **Shared Receptionist**

- Separate message pads for separate firms
- Separate database for separate firms
- Computer monitor visible to visitors
- Receptionist should be instructed to not take detailed phone messages.
 - Either write down only, _____ called. Please call _____, etc.
 - Or direct caller to leave a voice message on the voice mail box
- Receptionist should not open mail, then distribute it to tenants. Distribute the mail to tenants for them to open themselves. Same with hand-delivered items
- Messages: Do not share a Message Inbox with other tenants. Phone Messages taken by shared receptionist or support staff should be isolated and secure from other tenants, both during business hours and after. Treat all messages the same. Do not impose the responsibility upon receptionist or support staff to determine whether a phone message should be kept confidential or not.

Using a common receptionist as a “referral service.” (See **Opinion No. 2001-09** (October 2001), appended to the end of this section on Office Sharing.)

➤ **Awareness**

- At all times you should be aware that you are in the presence of others not a part of your firm
- Overhear your conversations: Personally? Telephonically?

Excerpt from CLE Presentation on “Setup office, office sharing, technology”
by Susan Traylor

- **Secure Oral and written Communications**
 - Do you talk about client matters in the hallway, in the kitchen, in the restroom?
 - Do you leave client written materials visible for others outside your firm to see?

- **Secretaries Sharing Common Work Area**
 - Protect work area when at work and away from desk.
 - Keep inbox/outbox in attorney's office
 - Files and documents should not be left out, unsecured, overnight.

- **Answering Machines**
 - Un-secured. Anyone can listen
- **Voice messages**
 - Are Secure. Do not give out password.
 - Do not play out loud. Pick up receiver and listen
- **Fax Machines**
 - Outgoing faxes: OK, so long as you or staff attends the fax as it is sent
 - Incoming: Problem, unless you instruct clients and others to call you before they send the fax so that you or staff can be by the fax machine to monitor it.
 - Solution: Computer Integrated fax service (Fax card): Fax is received on your computer as an image file.
 - Solution: Purchase inexpensive fax machine and place in private area, i.e. support staff area which is private, or in attorney's office which can be locked.

- **Files**
 - Shared File Room or Support Staff Desk
 - Only non-confidential client documents or ability to lock up at night the confidential files
 - In Attorney's office, which can be locked at night

- **Photocopying and Shared Printers**
 - Your client's confidential copying should always attended by you or your staff

- **Calendaring or Scheduling Shared Resources**
 - Many suites housing more than one firm use a master calendar for the purpose of scheduling resources shared by all, i.e. conference rooms, projectors, laptops, etc. Use your name only when documenting your reservation. DO not include confidentially client information visible to your Suite-mates.

- **Trust Account Records**

Arizona attorneys have a duty to “keep safe” client trust account records, ER 1.15. Although this rule does not specifically address the office sharing situation, it is recommended that when sharing a suite with other firms or businesses, the firm’s trust account checkbook be kept in either a locked drawer or office, and that the trust account records be maintained confidentially. (See Rule 42, Arizona Rules of Professional Conduct, ER 1.15 “Safekeeping Property”)

➤ **Technology:**

- **Passwords**
 - Use passwords at all times
 - Write down passwords to computer & voicemail in secure place known to attorney (Windows 2000 and newer allows for an Administrator password which will allow attorney to access the computer even without knowing the support staff’s password. This may not be possible for passworded databases, however, or voicemail.)
 - Routinely change passwords, i.e. every 3-6 months

- **Computer & Voicemail Passwords**
 - Password to logon to computer
 - Password to logon to computer network
 - Password to logon on to applications, especially databases and communications software, i.e. integrated faxing
 - Password to voicemail box

- **Tips re Passwords**
 - DO NOT GIVE OUT passwords (except staff to attorney)
 - Write down password on stickie at stick to computer monitor or anywhere visible
 - Easily decoded passwords are: family names, pet names, birthdates, maiden names

- **Networking Computers**
 - Option 1: If sharing a server with suite-mates
 - MUST HAVE “permissions and restrictions” properly configured on the file server
 - May have “permission” to share library resources, most forms resources, shared applications, internet service provider
 - Must “restrict” access on client digital files, firm e-mail, integrated fax mail
 - Must have qualified Network Computer Specialist to ensure proper security setup
 - Option 2: If purchase “dedicated computer” to act as server ONLY for your firm
 - MUST place it in secure room or space

Option 3: If using a “peer-to-peer” networking system, e.g. one of the multiple computers you have purchased for your firm “acts” as the server. It hosts all the shared files and data to be used by you and your staff.

- **Sharing a Database with Suite-Mates**

Do not do this. Although many sophisticated databases have the capability of being configured so that users can be “restricted and permitted” access as necessary, it simply is too dangerous and often too precarious to maintain properly.

- **Single Workstation**

If you are using “Go to My PC” or “PC Anywhere”, software or browser based products that allow you to log onto your computer from anywhere outside your office, so long as your computer is left on, beware to have that computer in a secure room or office.

- **Backups**

Keep backup tapes, CDs, diskettes secure from suite-mates. Use passwording on backups if at all possible (this secures the backups even when taken off-site)

- **Laptops / PDAs**

Don’t leave them laying around the office, accessible to your suite-mates Always use password your laptop or PDA. If necessary to leave them unattended, turn them off

- **Shredder**

Shredders are inexpensive. Even if your office space is isolated and secure from your suite-mates, using a shredder is a good way to dispose of discarded work product.

- **Policy and Procedures re Maintaining Confidentiality of Client Information**

- Make certain staff reads it and reviews