

Document Disposal: When and How to Throw It Out

Contributed by Victor O. Schinnerer & Company Inc.

Revised February 2007

The AIA collects and disseminates Best Practices as a service to AIA members without endorsement or recommendation. Appropriate use of the information provided is the responsibility of the reader.

CONSULT YOUR ATTORNEY

The information herein should not be regarded as a substitute for legal advice. Readers are strongly advised to consult an attorney for advice regarding any matter related to document retention or document destruction policies and practices.

SUMMARY

A desk filled with paper can become a nuisance and, as much as we want to just drop it in the recycle bin, a few considerations need to be taken into account first. This Best Practice proves that shredding is important and discusses what documents should not be thrown away and the correct disposal methods for those documents that can be thrown away.

SOME THINGS ARE NOT FOREVER

Every firm gathers information that should be destroyed after it is no longer needed for its original purpose. Document destruction helps maintain confidentiality of records or information that may be of a personal, proprietary, or competitive nature.

The information whose confidentiality you seek to protect through destruction may be the property of the firm, but more often it is information that belongs to others, such as employees or clients. A document destruction policy, consistently implemented, may be as important as a firm's document retention policy.

The type of information to consider for destruction includes, but may not be limited to, the following:

- Confidential information from clients, particularly strategic business information
- Information about employees, particularly medical or insurance claim information
- Drafts of documents and correspondence
- Memoranda or other documents that contain business information about the firm that might interest competitors

Every firm is entrusted with information about its employees that must be kept private; in fact,

employees have a legal right to protection of some information, particularly medical information.

Equally important, the firm may have a duty, which may be a contractual duty, to protect confidential information received from clients.

Finally, the firm may possess some information that competitors or others simply should not see. Securely collect and destroy incidental records such as phone messages, memos, and drafts.

WHAT TO KEEP

Project record documents must be maintained as long as necessary to provide for a proper defense if a professional liability claim is made against the firm. Other documents may also need to be retained, but it is neither necessary nor wise to retain every document created by or flowing through a professional service firm.

DEVELOP AND ENFORCE A POLICY

Develop a policy for document destruction that is based on sensible criteria and logical methods. Develop a timetable for destruction of specific types of documents, and adhere to the schedule.

A well-developed retention schedule will take into account the value of a record to the firm and any governing legal requirements. A contractual commitment to a client may define a specific retention and/or destruction obligation.

DESTROY COMPLETELY

Document destruction should be total and absolute. Destroy documents in a way that ensures, and confirms, that the information is obliterated before the documents leave the firm's possession—for example, by shredding before disposal.

Without proper safeguards, information could end up where it could be readily, and legally, available to anyone. Recycling or disposing of records may not be sufficient. Trash can be the single most available source of competitive and private information from and about a firm. Once a recycling company obtains

wastepaper, that company has no obligation to keep information confidential.

If private and proprietary data is discarded without being obliterated, a firm exposes itself to the risk of criminal and civil prosecution as well as embarrassment and the potential loss of business.

RETAINING INFORMATION FOR LITIGATION

A firm that destroys documents without a program of routinely destroying records exhibits suspicious disposal practices that could be negatively construed in the event of litigation.

Even if a policy is set and routinely followed, documents important to a dispute resolution process or government action must be preserved.

If there is an investigation and relevant documents have been intentionally destroyed, the firm could be found guilty of obstruction of justice.

If a contractual dispute or third-party claim is brought against a firm, scheduled document destruction may have to stop.

The Federal Rules of Civil Procedure require that each party provide all relevant records to opposing counsel within 85 days of the defendant’s initial response. Evidence of the destruction of documents that might be subject to this discovery rule could result in legal sanctions and lost credibility. By destroying stored records according to a set schedule, a firm limits the amount of material it must search through to comply with discovery rules.

Documenting the exact date that a record is destroyed is a prudent and recommended legal precaution.

THE RECORD DESTRUCTION PROCESS

While a firm may have a fiduciary duty to its employees and a contractual privacy obligation to its clients, there is no fiduciary responsibility inherent in the recycling of paper.

With paper recycling there is no practical means of establishing the exact date that a record is destroyed. In the event of litigation, this could be a legal necessity. If something of a private nature surfaces, the selection of an unsecured destruction process could be interpreted as negligent.

A firm cannot transfer its responsibility to maintain confidentiality to its employees and clients. Common sense dictates that payroll information, materials that involve legal affairs, and competitive information should not be entrusted to lower-level employees for destruction.

Many construction-related professional service firms tend to keep information far beyond its usefulness. When they eliminate their stored information, they often do so casually.

If proprietary or private information is lost by the negligence of a firm or leaked through the fraud of an employee, disastrous results could occur, such as employment practices claims, loss of business, initiation of legal action by a client, prosecution by civil authorities, or troublesome negative publicity.

RESOURCES

More Best Practices

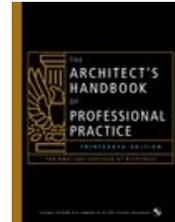
The following AIA Best Practices provide additional information related to this topic:

- 10.01.02 The Paperless Office
- 10.01.03 Project File Organization
- 10.01.04 Quality Control: A Project Record Retention Checklist

For More Information on This Topic

See also “Information Management,” by Elena Marcheso Moreno, *The Architect’s Handbook of Professional Practice*, 13th edition, Chapter 13, page 380.

See also the 14th edition of the *Handbook*, which can be ordered from the AIA Bookstore by calling 800-242-3837 (option 4) or by email at bookstore@aia.org.



Feedback

The AIA welcomes member feedback on Best Practice articles. To provide feedback on this article, please contact: bestpractices@aia.org.

Keywords

- Practice. Information management
- Office information resources
- Office archives, Records retention plan



Two Wisconsin Circle
Chevy Chase, MD 20815-7022
(301) 951-9746
www.planetAEC.com

This Best Practice is a contribution of Victor O. Schinnerer & Company, program administrators of the AIA Commended Professional Liability Insurance Program. Adapted with permission from Schinnerer’s Guidelines for Improving Practice.