Destruction of Public Records: A Procedural Guide

Contents

Summary

These procedures are for personnel in Kentucky state and local government agencies who are responsible for arranging for the authorized destruction of records. This guide provides sound, practical advice on physical destruction of records, regardless of format.

1.0 Introduction

1.1 Definitions

Appraisal is the process of determining the value and then the disposition of records based on their current administrative, legal and fiscal use; their evidential and informational or research value; their arrangement; and their relationship to other records.

Clearing of data is a process of deleting files using specialized software that removes information from storage media in a manner that renders it unreadable, unless special utility software or techniques are used to recover the cleared data. Clearing is a low-level form of overwriting (see overwriting.)

Commission is the State Libraries, Archives, and Records Commission, defined in KRS 171.410 (3) and 171.420.

Confidential Information is that information or data exempted from public disclosure under Kentucky's Open Records Act. These exemptions are listed in KRS 61.878 (1).

Department is the Kentucky Department for Libraries and Archives, defined in KRS 171.410.

Disposition is the action taken with regard to non-current records following their appraisal. These actions might include transfer to the State Records Center for temporary storage; transfer to the State Archives for permanent preservation; maintain in agency; reproduce on microfilm; or destroy.

Division is the Archives and Records Management Division, Kentucky Department for Libraries and Archives.

Expunge (expunging, expunged) is the process of permanently removing or destroying all or parts of a record, usually under a court order. In some cases, expunge refers to the process of sealing a record, or restricting access to the record in question.

Media is the material used for the storage of information or data.

Overwriting is a software process that replaces the data previously stored on magnetic storage media with a predetermined set of meaningless data. Also referred to as reformatting

Public agency, defined in KRS 171.410 (4), is

- every state or local office, state department, division, bureau, board, commission and authority;
- every legislative board, commission, committee and officer;
- every county and city governing body, council, school district board, special district board, municipal corporation, and any board, department, commission, committee, subcommittee, ad hoc committee, council or agency thereof; and
- any other body which is created by state or local authority and which derives at least twenty-five percent (25%) of its funds from state or local authority.

Public record or **record**, defined in KRS 171.410 (1), is documentary material, regardless of physical format, which is prepared, used or retained by public agencies in connection with regular agency business.

Records inventory or **inventory** is a list identifying the location, name and description of each records series, held by a state or local government agency. A completed inventory provides information essential to preparing a records retention schedule, with appropriate retention and disposition instructions, for records created and maintained by a state or local government agency.

Records officer, defined in 725 KAR 1:010, is the public agency employee who represents a unit of government in its relations on records management issues with the division.

Records series is a file unit or group of documents related to a particular subject or function, resulting from the same activity, having a common form, or having another relationship in their creation, receipt or use.

Records series number or **series number** is a unique identifying number assigned to each records series on a records retention schedule.

Removable media is a type of computer media designed to be portable and allow for easy transfer of data from one device to another.

Retention period is the minimum length of time a record is to be maintained in an accessible format. Records may be maintained at the creating agency or at an approved archives or records storage facility.

Retention schedule or **schedule** is a document governing the retention and disposition of records series of a state or local public agency. A schedule contains a list of the various records or records series created, used or maintained by a public agency, together with information about the specific periods of time during which records must be maintained and disposition instructions to be applied to the series when its business use has ended.

Sanitizing is the process of removing the data on computer media before the media is reused in an environment that does not provide an acceptable level of protection for the data. In general, laboratory techniques cannot retrieve data that has been sanitized/purged.

1.2 Legal requirements

The destruction of public records is subject to the terms of **KRS 171.410-740** (*the State Archives and Records Act)*, in conjunction with **725 KAR 1:030** (*Disposal or destruction of public records; procedure*). Under the statute, there are a number of ways to legally dispose of public records:

- with the permission of the Commission, through the application of General Retention Schedules, covering common classes of records created by public agencies, or of agency-specific Retention Schedules, covering the records that document the role of a particular public agency; and
- under provisions of certain legislation that authorizes the destruction of certain records.

By nature of the powers inherent to judiciary in the state constitution and by common law, the judicial branch has the power to order records destroyed in a variety of situations.[1] (see section 2.1.3 Expunging Records below)

Any questions of uncertainties about proper approval for records destruction should be directed to the Division.

---

[1] *Ex Parte Farley,* Ky., 570 S.W.2d 617 (1987) and *Bowling v. Sinnette,* Ky., 666 S.W.2d 743 (1984)

1.3 Penalties

Under the terms of **KRS 519.060 (1) (b),** a person who *"intentionally destroys, mutilates, conceals, removes, or otherwise impairs the availability of any public records"* without the authority to do so is guilty of tampering with public records, a Class D felony.

1.4 Summary of process

Before records destruction can occur, the following must take place:

- the records have been authorized for destruction in accordance with the requirements of an approved Records Retention Schedule;
- there is no active or pending litigation, audit, Open Records request, or appeal of an Open Records decision, that involves the records in question;
- the records are no longer required under any other legislation, and all statutory and regulatory requirements are fulfilled;
- the records are of no further administrative or business use to the agency; and
- a Records Destruction Certificate has been completed and signed by the appropriate authority.

Then the records must be destroyed in an appropriate manner.

2.0 Principles of Destruction

Records destruction should be:

- authorized,
- appropriate,
- secure/confidential,
- timely, and
- documented.

2.1 Authorized

There are at least two levels of authorization required for the destruction of records:

- formal destruction authorization by the Commission, by an approved Records Retention Schedule, together with completion of a Records Destruction Certificate; and
- internal authorization through the agency's internal approval process.

2.1.1 Authorized by the State Libraries, Archives, and Records Commission

Approved Records Retention Schedules provide state and local government agencies with the formal authorization to dispose of eligible public records. The schedule sets the *minimum* period for retention. A record authorized for destruction in an approved and current retention schedule may be destroyed at the end of the appropriate retention period. For advice on applying retention schedules to records, contact the State or Local Records Branch, Archives and Records Management Division, KDLA.

2.1.2 Authorized by Organization

While Records Retention Schedules set a minimum period for retention, it is also important to ensure that the organization has no further business or legal needs for particular records. This can be done by ensuring that there are appropriate internal authorization or approval processes in place (for example, by providing appropriate staff with lists of records due for destruction).

A public agency must not dispose of any records required for current or pending legal action or where the records may be required as evidence in a court case. An agency must not destroy records that are the subject of a current or pending Open Records request or an administrative or judicial appeal of an Open Records decision.

Once all requirements for retaining records have been met, the agency's Records Officer should give the final internal approval for the destruction of records. Each organization should ensure that a Records Officer has been named and made responsible for this process and that the Division has been advised of the designee.

2.1.3 Expunging records

In certain instances, Kentucky law allows for the courts, or other administrative bodies, to order that records be expunged, or sealed. In most cases, when the courts order that record(s) be expunged, the agency holding the records can delete all references to the record(s) in question and may legally deny their existence. The agency is then required to protect that record in such a way that prohibits the information from disclosure. There are instances in which the court could order the record to be reopened at a later date. While the expungement order affects access to the record(s) in question, agencies should continue to follow the retention period listed in the appropriate Records Retention Schedule, unless ordered differently by the court.

2.2 Appropriate

Appropriate methods for destruction are:

- Irreversible and
- environmentally friendly.

Suitable methods of destruction for different media are covered in 3.0, *Methods of Destruction* section.

2.2.1 Irreversible

Destruction of records should be irreversible. This means that there is no *reasonable risk* of the information being recovered again. Failure to ensure the total destruction of records may lead in some cases to the unauthorized release of confidential information.

A number of cases have been reported in the media where records have been found "unearthed" in local landfills after they had been buried or left in cabinets that had been sold as surplus. Records have also been found on the hard drives of government computers that have been sold. Such events reflect poorly on public agencies and the Commonwealth of Kentucky as a whole and could lead to adverse legal action.

2.2.2 Environmentally friendly

Records should be destroyed in an environmentally friendly manner. Both paper and microforms should be recycled when possible.

When disposing of computer equipment or other hardware, agencies must take appropriate measures to remove all hazardous waste components (circuit boards) and to destroy the fixed disk unit. With the hazardous waste removed, these elements may be discarded as solid waste.

2.3 Secure/Confidential

Records should always be disposed of with the same level of security that was maintained during the life of the records. Wherever possible, destruction of records should be supervised by an officer of the agency or by another authorized agent if destruction has been contracted out.

Extra care should be given to records containing confidential information (see also 5.0, *Confidential Information* section).

Lockable [bins may be used for particularly confidential records. Confidential records that are not binned should be transported in totally enclosed and lockable vehicles (to prevent records falling off the back of trucks!) and destroyed in the presence of an officer of your agency (or an authorized representative – see section 4.0, *Using a Contractor*, for more information). Confidential records may also be shredded “in-house” before being sent for recycling. Any in-house shredding should still be approved through the normal internal and external approval processes.

2.4 Timely

While records should not be destroyed while there is still a need for them, it is also important not to keep records longer than necessary, in order to minimize storage costs and increase retrieval efficiency. Records destruction is a natural part of the life cycle of records. Records are created, pass through a useful life, and are then disposed of when they are no longer needed by the agency – according to the Records Retention Schedule. This life cycle is part of the business process, and destructions must occur on a regularly scheduled basis. An established procedure for destroying records at specific intervals is necessary. A good time for destruction *usually* occurs at the end of a calendar or fiscal year, at the end of an audit cycle (following publication of the audit report), or at the end of

a contract or grant project. It may also be helpful to have periodic “records maintenance” or “clean-out” days in which employees are encouraged to go through their files (both paper and electronic) and remove material that has exceeded its scheduled retention period. **Note: The retention periods listed in the records retention schedule, and any internal destruction, must still be followed.**

If a decision is made to retain records longer than the minimum retention period, a record of the reasons for the decision should be documented to assist destruction at a later date.

2.5 Documented

2.5.1 Records Destruction Certificates

The destruction of all records must be documented, so that each agency is able to determine whether a record has been destroyed. Proof of destruction may be required in legal proceedings or in response to Open Records requests. This proof is provided by a Records Destruction Certificate.

The Division requires agencies to complete a Records Destruction Certificate when destroying records. Records Destruction Certificates are available from KDLA’s website at: http://www.kdla.ky.gov/.

The Records Destruction Certificate records the:

- series number and title of each series destroyed,
- date of destruction,
- date span of the records series destroyed,
- volume of the records destroyed, and
- method of destruction.

The Records Destruction Certificate is completed and signed by the agency Records Officer before a copy is sent to KDLA. A copy is also filed in the agency, together with any other destruction documentation (for example, records of internal approvals).

2.5.2 Certification of Sanitization (for state agencies)

Computer hard drives must be destroyed when they are defective or cannot be repaired or sanitized for reuse. Physical destruction must be accomplished to an extent that precludes any possible further use of the hard drive. (For more information about destroying hard drives, see section 3.2, *Methods of Destruction, Electronic Media.*)

The Finance and Administration Cabinet's Division of Surplus Property requires that a copy of the proof of sanitization accompany all hard drives earmarked for destruction. Prior to submitting surplus forms (*B217-2: Declared Surplus*) from the Finance and Administration Cabinet's Division of Surplus Property to the agency's appropriate organizational unit, the sanitizing process must be documented on an additional form that explicitly outlines the method(s) used to remove data from the storage media, the type of equipment/media being sanitized, the name of the individual requesting sanitization, and the name of the person responsible for the sanitization. A template for the form is the *Commonwealth of Kentucky Record of IT Equipment Sanitization* that contains the elements required by the Division of Surplus Property. A completed record (including the top section) must be maintained in a central location designated by the agency. This information must be maintained as outlined by the approved Records Retention Schedule. For disposition other than to the Division of Surplus Property (such as interagency transfer), it is highly recommended that an adhesive label be affixed to the equipment case to record the sanitization process before transfer.

For more information, see the Enterprise Policy CIO-077, Sanitization of IT Equipment and Electronic Media.

3.0 Methods of Destruction

There are a number of different methods of destruction appropriate to the different media on which the records are stored.

3.1 Paper records

3.1.1 Shredding

The security provided by the shredding of records depends on how fine the paper is shredded. Cross shredding may be needed for particularly sensitive documents.

3.1.2 Recycling

Kentucky state government has a program to recover recyclable paper from offices in Frankfort. The program, administered by the Kentucky Division of Waste Management (DWM), provides different levels of service depending on the location of offices. The State Office Paper Recycling Program is managed by the Kentucky Government Recycling Section in DWM. DWM provides Frankfort offices with containers for white office paper, and the collecting agencies provide the containers for newsprint and mixed paper. Employees should separate material at their workspaces and then periodically place it in the appropriate collection container.

Each cabinet in state government has a coordinator who distributes information and assists in educating employees about the program. The DWM employees then collect the material on a regular basis in each of the state office buildings. The material is transported to a warehouse where it is sorted, baled, and loaded for shipment to a private contractor in Lexington.

State offices outside Frankfort are required to institute recycling programs to recover office paper, where practicable. State-supported colleges and universities are required to develop programs to recover office paper.

For more information, please refer to the Kentucky Government Recycling Section, located on the Department of Environmental Protection's website.

3.1.3 Burning

Records should only be burnt if there is no environmentally friendly method of destruction available. Records should be burned in accordance with any environmental guidelines and local burning restrictions. Densely packed paper does not burn well, so burning should be undertaken in an industrial facility (not in a "backyard" incinerator).

Important: Burying is not an appropriate method of destruction for sensitive or confidential records. The records are not destroyed immediately and may take months or even years to break down. Records that are buried may also be uncovered within hours or days of being buried.

3.2 Electronic Media

It is a common belief that information is destroyed when files are erased or deleted, although all that is normally removed are the logical pointers to the information. Simply deleting files or even formatting the hard drive(s) does not prevent subsequent recovery and use of this information by using commonly-available applications. Sanitization is the process by which data is removed from information technology equipment and storage media and rendered unrecoverable. In general, laboratory techniques cannot retrieve data that has been sanitized.

The following section outlines the acceptable methods to remove data from storage media. When a computer is surplused or given to a new user within an agency, sanitization must be performed to ensure that information is removed from the hard drive in a manner that gives assurance that the information cannot be recovered. Before the sanitization process begins, the computer must be disconnected from any network to prevent accidental damage to the network operating system or other files on the network.

There are two acceptable methods to be used for the removal of records from electronic media:

- Overwriting
    - Physical Destruction

The method used for removal depends upon the future use of the media:

- Media (hard drives, rewritable disks, etc.) that will be reused should be overwritten. If the operable hard drive is to be removed from service completely, it should be physically destroyed or sanitized according to the

Enterprise Policy CIO-077, Sanitization of Information Technology Equipment and Electronic Media.

- If the hard drive is inoperable or has reached the end of its useful life, it should be physically destroyed.

3.2.1 Overwriting

Low level overwriting or clearing of data is a process of deleting files using a specialized program that removes information from storage media in a manner that renders it unreadable, unless special utility software or techniques are used to recover the cleared data.

There are a large number of products with widely varying price structures available, and it is imperative that any selection made adheres to the Department of Defense standard and:

- Supports any size hard drive;
- Permanently erases operating systems, program files, and data;
- Erases ALL data from the physical hard drive; and
- Erases all partition tables and drive formats.

Low level overwriting is a process that is best used for the removal of data from computers that will continue to be used within the agency. **Note: Because the low level overwriting process does not prevent data from being recovered by technical means, it is not an acceptable method of sanitizing hard disk storage media that will be resold or discarded.**

High level overwriting (reformatting) of data means replacing previously stored data on a drive or disk with a predetermined pattern of meaningless information. This effectively renders the data unrecoverable. Software products and applications used for the overwriting process should meet the following specifications:

- The data must be properly overwritten with a pattern.

- Sanitization is not complete until three overwrite passes and a verification pass are completed.
- The software should have the capability to overwrite the entire hard disk drive, making it impossible to recover any meaningful data.
- The software must have the capability to overwrite using a minimum of three cycles of data patterns on all sectors, blocks, tracks, and any unused disk space on the entire hard disk medium.
- The software must have a method to verify that all data has been removed.
- Sectors not overwritten must be identified.

3.2.2 Physical Destruction

Hard drives should be destroyed when they are defective or cannot be repaired or sanitized for reuse. Physical destruction must be accomplished to an extent that precludes any possible further use of the media. This can be attained by removing the hard drive from the cabinet and removing any steel shielding materials and/or mounting brackets and cutting the electrical connection to the hard drive unit. The hard drive should then be subjected to enough physical force or extreme temperatures that will disfigure, bend, mangle or otherwise mutilate the hard drive so it cannot be reinserted into a functioning computer.

3.2.3 Removable Media

Due to the relatively low cost of removable storage media, the best advice for all media that cannot be reused is to physically destroy the media. The state Division of Waste Management has more information on their website.

3.2.3.1 Magnetic Media (tape, floppy disk)

Records stored on magnetic media can be reformatted. Reformatting is a process of deleting files using a specialized program that removes information from the media in a manner that renders it unreadable, unless special utility software or techniques are used to

recover the cleared data. There are a large number of utility products with widely varying price structures available. Reformatting is a process that is best used for the removal of data from media that will continue to be used within the agency.

Note: Because the reformatting process does not prevent data from being recovered by technical means, it is not an acceptable method for storage media that will be resold or discarded.

Remember: Do not just delete files from electronic media, such as floppy disks, rewritable optical disks and hard disks, as the information can be recovered.

3.3 Other Non-Paper Media

Videos, cinematographic film and microforms (microfilm/ fiche/ aperture cards/ x-rays) can be destroyed by shredding, cutting, crushing or chemical recycling.

4.0 Using a Contractor

4.1 Responsibilities

Contractors may be hired to destroy records. Even in a contracting situation, it is the responsibility of the agency to ensure that destruction occurs in accordance with the approved methods of destruction.

4.2 Transport of records

The contractor can collect records from your office for destruction, or you can deliver the records to the contractor. A closed truck should be used whenever possible. If there is no alternative and the contractor can only provide an open truck, however, ensure that the load is secured by a cover. Sensitive and confidential records should only be conveyed in a closed and lockable vehicle.

4.3 Documentation

Always insist on a certificate of destruction from the contractor. If records that were supposed to be destroyed are subsequently found, the certificate is evidence that the contractor was at fault, not your organization. You may also want to request that the certificate of destruction include the method used. Agencies still need to complete the KDLA Records Destruction Certificate, even if using a contractor.

5.0 Confidential Information

Records maintained by public agencies frequently contain information that may be excluded from public inspection and will require special destruction measures. The Kentucky Open Records Law permits agencies to withhold records, or portions thereof, which fall within one or more statutory exemptions found at KRS 61.878(1). KRS 61.878(1)(k) and (l) direct agencies to withhold records made confidential by other state statutes or federal law. Agencies should exercise particular care in handling and destroying records containing protected information.

For more information on restricted information in public records, see: *Outline: The Law of Open Records and Open Meetings*, located on the Office of the Attorney General's website These statutes erect absolute barriers to disclosure of the affected records. Great care should be exercised to ensure that the protections they afford are not breached throughout the life of the records.

5.1 Sensitive Document Destruction Service (for state agencies)

DWM provides sensitive document destruction services for state agencies and state universities. Agencies need to follow these procedures for destruction services:

1. Inform employees that documents are manually fed into an industrial shredder and not incinerated. This seems to be a misconception among several agencies which may explain the large amounts of hazardous materials found in many boxes marked “burn”.
2. Designate a centralized, secure location for all sensitive documents to be destroyed, and move those documents to that location prior to scheduled collection time.
3. Ensure all non-paper items are removed from documents, including:
   a. metal fasteners;
   b. plastic binders;
   c. cardboard;
   d. food containers and wrappers;
   e. broken bottles and other hazardous materials; and
   f. microfilm, diskettes, and magnetic tape.
4. Place on pallets and stretch wrap documents prior to collection. The Kentucky Government Recycling Section will provide pallets as needed and training on how to properly stack and wrap pallets.
5. Request document destruction service a minimum of five working days prior to the desired date of destruction.
6. Designate a chain of custody representative to witness the destruction process (if required by agency security procedures).

1. Use the downloadable Records Destruction Authorization Form (found on the KDLA website).

Appendix A: Checklist for records destruction

	The records are authorized for destruction under a relevant and current Records Retention Schedule
	The agency no longer requires the records
	The records are not the subject of a current or pending court case or Open Records request
	Internal authorization has been obtained
	The records have no special security requirements OR The records have high security level and locked bins and/or in-house shredding are required for security destruction
	Appropriate service provider contacted
	A covered van/truck specified for records removal
	Service provider asked to supply certificate of destruction
	Specified that records are to be destroyed on day of collection
	Certificate received by organization
	Records destroyed and details of destruction documented in the organization's records system.