

What is the Freedom of Information Act 2000?

The Freedom of Information Act 2000 came into force on 1st January 2005. Among other things, it gives individuals the right to request information held by public authorities.

What documents are covered?

Emails, reports, research and minutes of meetings are all examples of information that can be requested by members of the public under the Act.

*There are 23 exemptions to the Act under which information does not have to be disclosed. Information relating to national security, information that would prejudice international relations, commercially sensitive information and confidential information is all exempt from the general rights of access. The exemptions are categorized into **absolute exemptions, qualified exemptions or exceptions**. The public authority must apply the public interest test where there is a qualified exemption or exception and this generally favours disclosure. The information may only be withheld if the public authority considers that the public interest in withholding the information is greater than the public interest in disclosing it.*

What is a public authority?

Public authorities covered by the Act include central and local government, hospitals, doctor's surgeries, dentists, opticians and pharmacists, state schools, colleges and universities, police forces and prison services. A full list is provided in Schedule 1 of the Act and the Secretary of State also has power to designate further public authorities under section 5 of the Act.

Records Management and Destruction

The Lord Chancellor has laid down a Code of Practice on the Management of Records under section 46 of the Freedom of Information Act 2000 and public authorities must also comply with their obligations under the Data Protection Act 1998.

The Code recommends that public bodies have clear information management policies and says that they should include the following:

- **Records Management as a Function.** *The records management function should be recognised as a specific function within an organisation and should receive the necessary levels of internal support to ensure effectiveness.*
- **Draft a Records Management Policy.** *Senior Management should distribute the completed Records Management Policy Statement to all staff in the organisation. This reinforces the importance that your organisation places on document management and also represents your organisation's official procedures regarding document management policies.*
- **Designated Role.** *A designated member of staff of appropriate seniority should have lead responsibility for records management within your organisation.*
- **Recruit Knowledgeable Staff.** *Human resource policies and practices in organisations should address the need to recruit and retain good quality staff for records management.*
- **Records Management System.** *Each department within your organisation should have an adequate system in place for documenting its activities. The records that are created should be arranged in a record keeping system that will enable you to obtain the maximum benefit from the quick and easy retrieval of information.*
- **Tracking Your Information.** *The record-keeping system, whether paper or electronic, should include a set of rules for referencing and indexing records. This is an effective method for tracking your information.*
- **Storing & Maintaining Your Records.** *The movement and location of records should be controlled to ensure that a record can be easily retrieved at any time and that there is an auditable trail of record transactions. Barcode tracking is an effective system for managing your information. Storage accommodation for current records should be clean, dry and secure. Equipment used for current records should provide storage which is safe from unauthorised access and which meets fire regulations, but which allows maximum accessibility to the information.*

- **Business Continuity.** A contingency or business recovery plan should be in place to provide protection for records, which are vital to the continued functioning of the authority. Backing up critical business information and storing it off-site is core to any successful business continuity plan.
- **Record Closure.** Records should be closed as soon as they have ceased to be of active use other than for reference purposes.
- **Management of Electronic Records.** The principal issues for the management of electronic records are the same as those for the management of any record. They include, for example the creation of authentic records, the tracking of records and disposal arrangements.
- **Outsourcing.** It has now reached a stage that it is less common for files to be stored in house and more common for this function to be outsourced to professional record management companies. As the requirements of organisations grow more complex, the available solutions have become more sophisticated.
- **Training.** Adequate training of employees is essential so that everyone working in a public authority is familiar with the Freedom of Information Act and the criteria required to comply with it.
- **Disposing of Your Records.** It is particularly important under the Freedom Of Information Act that the disposal of records is undertaken in accordance with clearly established policies. Records that have reached the end of their administrative life should be destroyed in a secure manner.

Part 9 of the Code deals with secure storage and destruction of records. The relevant sections are as follows:

- 9.1 It is particularly important under the Act that the disposal of records is undertaken in accordance with clearly established policies which have been formally adopted by authorities and which are enforced by properly authorized staff.**



- 9.3** The storage of closed records awaiting disposal should follow accepted standards relating to environment, security and physical organisation.
- 9.8** Records not selected for permanent preservation and which have reached the end of their administrative life should be destroyed in as secure a manner as is necessary for the level of confidentiality or security markings they bear. A record of the destruction of records, showing their reference, description and date of destruction should be maintained and preserved by the records manager.

Environmental Information Regulations (EIR)

The EIR came into force on 1 January 2005, the same day as the Freedom of Information Act. It allows members of the public to request environmental information, but is wider than FOI in that requests for information can be made from some private companies and public private partnerships, most notably the utility and transport companies.

The Code of Practice on Records Management under s.46 of the Freedom of Information Act also applies to bodies subject to the EIR.

How can we help?

Securit works closely with its customers to ensure that materials are destroyed according to these standards. Securit can provide on-site shredding by its Customer Service Representatives, so its customers can easily monitor the destruction of their data. Upon completion, Securit provides a Certificate of Destruction which serves as a record that the documents were destroyed. For peace of mind, contact Securit today at 0800 028 1164.

For more information:

UK Information Commissioner – www.informationcommissioner.gov.uk

This document does not constitute a legal opinion or legal advice. Do not rely on any of the information in this document without first obtaining legal advice.

© Copyright 2005

Freedom Of Information Act - A Quick Reference Guide

Good Records Management has always been critical to the success of managing your information, but now that the **Freedom of Information Act 2000** has been fully implemented since January 1st, 2005, a sound Records Management policy is now a requirement for all public authorities.

The Lord Chancellor's Department has issued a Code of Practice under section 46 of the Act. This sets out good practice for records management. Arcane Filestores and Shred-it have prepared some helpful quick facts on the subject:

- **Records Management as a Function.** The records management function should be recognised as a specific function within an organisation and should receive the necessary levels of internal support to ensure effectiveness.
- **Draft a Records Management Policy.** Senior Management should distribute the completed Records Management Policy Statement to all staff in the organisation. This reinforces the importance that your organisation places on document management and also represents your organisation's official procedures regarding document management policies.
- **Designated Role.** A designated member of staff of appropriate seniority should have lead responsibility for records management within your organisation.
- **Recruit Knowledgeable Staff.** Human resource policies and practices in organisations should address the need to recruit and retain good quality staff for records management.
- **Records Management System.** Each department within your organisation should have an adequate system in place for documenting its activities. The records that are created should be arranged in a record keeping system that will enable you to obtain the maximum benefit from the quick and easy retrieval of information.
- **Tracking Your Information.** The record-keeping system, whether paper or electronic, should include a set of rules for referencing and indexing records. This is an effective method for tracking your information.
- **Storing & Maintaining Your Records.** The movement and location of records should be controlled to ensure that a record can be easily retrieved at any time and that there is an auditable trail of record transactions. Barcode tracking is an effective system for managing your information. Storage accommodation for current records should be clean, dry and secure. Equipment used for current records should provide storage which is safe from unauthorised access and which meets fire regulations, but which allows maximum accessibility to the information.
- **Business Continuity.** A contingency or business recovery plan should be in place to provide protection for records, which are vital to the continued functioning of the authority. Backing up critical business information and storing it off-site is core to any successful business continuity plan.
- **Record Closure.** Records should be closed as soon as they have ceased to be of active use other than for reference purposes.
- **Management of Electronic Records.** The principal issues for the management of electronic records are the same as those for the management of any record. They include, for example the creation of authentic records, the tracking of records and disposal arrangements.
- **Outsourcing.** It has now reached a stage that it is less common for files to be stored in house and more common for this function to be outsourced to professional record management companies. As the requirements of organisations grow more complex, the available solutions have become more sophisticated.
- **Training.** Adequate training of employees is essential so that everyone working in a public authority is familiar with the Freedom of Information Act and the criteria required to comply with it.
- **Disposing of Your Records.** It is particularly important under the Freedom Of Information Act that the disposal of records is undertaken in accordance with clearly established policies. Records that have reached the end of their administrative life should be destroyed in a secure manner.

For more information on how to develop a Records Management Policy or Document Destruction Policy please contact Arcane Filestores or Securit on telephone +028 9266 3535.

