Legislative Summary: Freedom of Information Act (FOIA)

Making sure it's secure.™

Freedom of Information Act (UK)

Enacted: November 2000; Into force: January 1, 2005

1 What the law covers:

- Any recorded information that is held by a public authority
- The public's right to access information that is held by public authorities

Access to information happens in two ways:

- The public authority is obliged to publish certain information about their activities
- Members of the public are entitled to request information

The Act does not give people access to their own personal data that is being held by the public authority. Access to this would be through a request under the Data Protection Act 1998.

2 Who must adhere to the regulations:

Public authorities that are based in England, Wales and Northern Ireland, and by UK-wide public authorities based in Scotland*.

They include:

- The Houses of Parliament, government departments and local authorities
- NHS hospitals, doctor's surgeries, dentists, opticians and pharmacists
- State schools, colleges and universities
- Police forces and prison services

*Scottish public authorities are covered by Scotland's own FOIA 2002

3 What is "recorded information":

Recorded information includes printed documents, computer files, letters, emails, photographs, sound or video recordings.

4 FOIA and information management:

The Lord Chancellor's Code of Practice on the Management of Records (the "Code") provides guidance to public authorities on how to comply with the FOIA.

They are required to:

- Recognise records management as a specific function that must be effectively managed
- Create a Records Management Policy that is endorsed by Senior Management and regularly reviewed
- Designate responsibility to a senior member of staff
- Train and give the necessary resource support to all staff
- Create an efficient and auditable records management system
- Securely back up and store all documents (paper and electronic)
- Establish document retention periods based on the types of information held
- Stipulate the methods of secure disposal
- Determine how to halt scheduled document destruction when a request for information is received

Other regulations to take into account: Data Protection Act and Environmental Information Regulations Act 2004.

For more information:

Information Commissioner's Officer – ico.gov.uk

Lord Chancellor's Code of Practice on the Management of Records under section 46 of the Freedom of Information Act 2000 – dca.gov.uk

Freedom of Information Act 2000 – opsi.gov.uk

Environmental Information Regulations 2004 – opsi.gov.uk

5 How to comply:

1. Under the FOIA, every public authority must have a publication scheme, approved by the Information Commissioner's Office (ICO), and publish information in accordance with the scheme. The ICO's guidance sets out what type of information, why it must be published and how much can be charged.

2. Requests for information held by a public authority from a member of the public must be treated equally.

Instances when a request can be refused:

- It would cost too much or take too much staff time to fulfill the request
- It is vexatious or contains personal data
- It repeats a previous request from the same person
- It falls under one of 24 exemptions (absolute or qualified)

6 Offences/penalties for non-compliance:

Members of the public can file a complaint with the ICO if they feel that an authority has failed to respond correctly to a request for information. If the Act has been breached, the resulting ICO decision notice will identify the remedial actions the authority must take.

Actions that may be considered breaches include:

- Failure to respond adequately to a request for information
- Failure to adopt the model publication scheme, or to publish the correct information

The ICO can still enforce compliance without a complaint. It can also issue an enforcement notice in either of the above instances or if an authority is repeatedly failing to comply with its obligations, e.g. taking too long to respond to requests.

A breach under Section 77 is a chargeable criminal offence:

- It covers the act of deliberately destroying, hiding or altering requested information to prevent it from being released
- The maximum penalty for the offending authority or individual is a fine of up to £5,000

7 Secure document retention and disposal guidelines:

Recommended inclusions for a records management policy:

- ☐ A statement of purpose
- ☐ Categories of documents and how long they should be kept
- ☐ Definition of "document" and the format and length of time in which it is to be retained (electronic or hard copy)
- ☐ Guidance on creation of documents
- ☐ Members of staff designated to deal with the document management system
- ☐ Guidelines for ensuring all staff are trained on how to comply with the policies and procedures
- ☐ Methods of document destruction, including those carried out by third parties
- ☐ How to keep an accurate record of documents destroyed

8 How Shred-it can help:

Secure Document and Hard Drive Destruction

- Secure end-to-end chain of custody
- Certificate of Destruction after every service
- Tailored solutions to your organisation's needs

Advice and Expertise

- Trained experts in information security
- Provide a Data Security Survey at your organisation
- Helpful resources available at shredit.co.uk/resource-centre

For peace of mind, contact Shred-it today

0800 028 1164 | shredit.co.uk

Making sure it's secure.™