
The Financial Services Authority

Records Management Policy and Standards - RMPS



Contents

Part A – policy		
1	Records Management	4
2	Introduction	5
3	What does this policy apply to?	5
4	Who does this policy apply to?	6
5	Why do we need to manage records?	6
6	Regulatory environment	7
Part B - roles and responsibilities		
1	Introduction	8
2	Executive responsibility	8
3	Information and Records Management Team (IRM) responsibilities	8
3.1	Policy and standards	8
3.2	Communication and awareness	9
3.3	Advice and guidance	9
3.4	‘Orphan’ records	9
4	Line management responsibility	9
5	Responsibility for project records	9
6	Responsibilities of individuals	10
Part C - standards		
1	What are records?	11
1.1	What is an ‘authentic’ record?	12
1.2	What is a ‘reliable’ record?	13
1.3	What is the ‘integrity’ of the record?	13

1.4	What makes a record 'useable'?	13
2	How do I decide what is a record?	15
2.1	Version control	16
3	Why do we need to 'capture' records?	16
3.1	Why do we need to 'register' records?	17
4	How long do I need to keep a record?	18
4.1	What is a 'vital' record?	19
5	What are subject classification & indexing? And why are they necessary?	20
5.1	What is a subject classification system?	20
5.2	What is an index?	21
5.3	What is vocabulary control?	21
5.4	Why use number and codes as well as using titles?	21
6	How do I store and handle records?	21
7	Access and security of stored records	22
8	Why do I need to keep track of records?	24
8.1	When should I use 'action tracking'?	24
8.2	Why do I need to keep track of a record's location?	25
9	When and how do we dispose of records?	25
	Part D	
	Glossary of terms	27
	Part E	
	References and links	29
	Part F	
	Security markings	30
	Annex A	
	FSA Retention Schedules	37
	Annex B	
	Recommended Retention & Disposal practices	50

A Policy

Having accurate and relevant information is vital to the efficient management of the FSA and we value records and information as corporate assets. We need to balance our statutory obligations (for example providing the public with information) and our desire to be open and responsive (in line with FSA Vision and Values) with our duties of confidentiality for personal and commercially sensitive records. So, we will create and manage all records efficiently, make them accessible when needed, but protect and store them securely and dispose of them safely at the appropriate time.

We will comply with all relevant legislation and aim to achieve standards of best practice. This will include adopting principles from such recognised bodies as the British Standards Institute (BSI) and the International Organization for Standardization (ISO).

We will make sure that staff have access to records management training. We will encourage staff to manage records properly.

We will provide supporting standards, procedures and guidelines. We will then state how compliance will be monitored. We will review our policy regularly to ensure it continues to be relevant.

1 Records Management

Good records management relies on the following principles being applied:

- the regular review of information
- the controlled retention of information
- the controlled destruction of information

Good management of records and the information contained within them will benefit the FSA through:

- records being easily and efficiently located, accessed and retrieved
- information being better protected and stored more securely
- records being disposed of safely and at the right time

The principle of records management is to ensure that a record is managed through its full Records Life Cycle i.e. the creation or receipt of a record, maintenance of the record, managing its use, access to it, storage, retrieval and finally disposal of the record.

2 Introduction

We are required by law to manage our records properly; statutes such as the Data Protection Act 1998 (DPA) and the Freedom of Information Act 2000 (FOIA) are particularly relevant, as they set out specific requirements on the creation and management of records.

A list of other Acts with links to them can be found in this Policy under section 6 - Regulatory environment. There are also links on Connect under records management.

This policy aims to make sure that all FSA staff and other users of FSA records understand what they must do to protect and manage records effectively, efficiently and economically.

This policy is supported by a set of records management standards, which we must all follow. These standards:

- set out how to manage FSA records and what tools to use;
- measure compliance of existing and evolving Divisional and Departmental records management practices;
- identify and promote best practice; and
- support the increased use of electronic records to gain operational benefits without introducing extra risks.

The policy is based on the international standard for records management ISO 15489. However, each Business Unit/Division/Department is responsible for developing working procedures for the day-to-day management of their records.

3 What does this policy apply to?

This policy and the standards that go with it apply to the management of records, in all technical or physical formats or media, created or received by the FSA while carrying out its business activities.

Although not an exhaustive list, examples of items that can be records include:

- documents (including written and typed documents and annotated copies);
- paper based files;
- computer files (including word processed documents, databases, spreadsheets and presentations);

- electronic mail messages (email);
- diaries;
- faxes;
- brochures and reports;
- intranet and internet web pages;
- forms;
- seized evidence;
- audio and video tapes, including CCTV
- microfiche and microfilm;
- maps and plans; and
- photographs

4 Who does this policy apply to?

This policy and the standards that go with it apply to all permanent and temporary employees, contractors, consultants and secondees who have access to FSA records, wherever these records are and whatever form they are in.

5 Why do we need to manage records?

Maintaining efficient records management practices will help us meet our statutory objectives and overall business responsibilities as a world class regulator. Whatever form the record takes, knowledge and information must be protected. It must also be accurate, ordered, complete, useful, up to date and accessible whenever it is needed to:

- a) help us carry out our business;
- b) make sure we comply with relevant legislation (see section 0 below);
- c) support theme work, research and development;
- d) help us all make informed decisions;
- e) keep track of policy changes;
- f) ensure that legal precedents are identified;
- g) support continuity and consistency in management and administration;
- h) protect the rights of employees, regulated entities and the general public;
- i) provide an audit trail to meet business, regulatory and legal requirements;
- j) make sure that we work effectively as a regulator and prosecuting authority and meet our lawful obligations for disclosing evidence;

- k) promote our activities and achievements; and
- l) make sure we are open and responsive, as set out in our Vision and Values and as required under FOIA <http://connect/corporate/vision/> & http://connect/corporate/vision/our_values.html#.

6 Regulatory environment

We work in a regulatory environment influenced by many factors:

- a) Statute, case law and regulations govern our business environment; these include, but are not limited to:
 - i. Financial Services and Markets Act 2000, in particular s.394 and Schedule I paragraph 9;
(http://connect/fsma/data/fsma/act/act_index.htm)
 - ii. Data Protection Act 1998;
(<http://www.hmso.gov.uk/acts/acts1998/19980029.htm#aofs>)
 - iii. Freedom of Information Act 2000¹;
(<http://www.hmso.gov.uk/acts/acts2000/20000036.htm#aofs>)
 - iv. Environmental Information Regulations 1992 & Environmental Information (Amendment) Regulations 1998;
 - v. Criminal Justice Act 1988;
 - vi. Civil Evidence Act 1995;
 - vii. Regulation of Investigatory Powers Act 2000 (RIPA);
 - viii. Companies Acts 1985, 1989; and
 - ix. The Human Rights Act 1998.
- b) Mandatory standards of practice, for example Company Law requirements.
- c) Voluntary codes of best practice, for example the Lord Chancellor's Code of Practice on the Management of Records under Freedom of Information (<http://www.dca.gov.uk/foi/codemanrec.htm>).
- d) Voluntary codes of conduct and ethics, which include, but are not limited to:
 - i. FSA Vision and Values; and
 - ii. FSA Code of Conduct (Conflicts of Interest, Share Dealing, Acceptance of Gifts and Hospitality).
- e) The expectations of our stakeholders and the community at large about what constitutes acceptable behaviour for the FSA.

1 The Freedom of Information Act 2000 came fully into force on 1st January 2005

B Roles and responsibilities

1 Introduction

The FSA owns all records created by employees² carrying out FSA business-related activities. Unless the originator keeps ownership (for example records seized as evidence during an enquiry) records received by FSA employees are also owned by the FSA. Individual employees do not own records but they do have responsibilities for managing records.

This document describes the roles and responsibilities for managing records within the FSA.

2 Executive responsibility

Members of the Chairman's Committee (now ExCo) have overall executive responsibility for our records management policy and standards, and for supporting their application throughout the organisation. Individual Directors have responsibility for ensuring that local procedures are in place and that records management; including review, file tracking, destruction is carried out in accordance with those procedures.

3 Information and Records Management team (IRM) responsibilities

The Information and Records Management team, part of Knowledge Management, has the following responsibilities:

3.1 *Policy and standards*

The IRM is responsible for making sure that the records management policy and standards are kept up to date and relevant to the needs and obligations of the organisation. They achieve this by consulting and working with FSA staff.

² This also applies to contractors/consultants/agents working on behalf of the FSA on FSA business.

3.2 Communication and awareness

The IRM is responsible for telling staff about the records management policy and standards and for ensuring that all staff are aware of their responsibilities for managing records.

3.3 Advice and guidance

The IRM is responsible for giving records-management advice and guidance to line managers, or their delegated records management staff.

3.4 'Orphan' records

The IRM is responsible for seeking decisions about the management of records for which there is no clear Business Unit responsibility, for example records for entities that are no longer regulated by the FSA.

4 Line management responsibility

Managers at all levels are responsible for:

- developing and operating records management procedures, covering both electronic and hard copy records, that:
 - are efficient and fit for purpose; and
 - comply with our records management policy and standards;
- ensuring that appropriate resources exist within the area for fulfilling the responsibilities for managing records;
- communicating local records management procedures;
- quality assurance of Divisional records management processes and procedures;
- ensuring that staff follow procedures for the offsite storage of hard copy records;
- ensuring that staff follow procedures for the management and storage of electronic records; and
- creation and maintenance of retention schedules and regular review and authorised destruction of records is carried out.

5 Responsibility for project records

Records about projects, which involve two or more Divisions ('horizontal projects') are the responsibility of the project manager. Project managers are responsible for:

- identifying project related records and liaising with relevant local contacts to ensure that the records are managed efficiently and comply with our records management policy and standards;
- ensuring that there are appropriate resources within the project for fulfilling the responsibilities for managing records;
- quality assurance of records management processes and procedures within the project; and
- ensuring the appropriate disposition of project records.

6 Responsibilities of individuals

Everyone who creates or receives records is responsible for following FSA and Divisional records management procedures.

C Standards

1 What are records?

Description

Records are defined as ‘information created, received and maintained as evidence and/or information by an organisation or person, in pursuance of legal obligations or in the transaction of business’.

Standards

A record should correctly reflect what was communicated or decided or what action was taken. It should also be able to support the needs of (have a useful purpose in) the business to which it relates and be used for accountability purposes. For example minutes should provide an accurate record of the decisions taken at a meeting.

As well as the content, the record should contain, or be linked to or associated with, the metadata, or context necessary to document a transaction, in the following way:

- The structure of a record, that is, its format and the relationships between the elements comprising the record, should stay intact.
- The record should clearly reflect the business context in which it was created, received and used. This should include the business process of which the transaction is part, the date and time of the transaction and the participants in the transaction, in other words an audit trail of the transaction.
- There should be links between items that are held separately but combine to make up one record, for example a spreadsheet in a PowerPoint presentation.

Records management procedures and practices should result in records which have authenticity, reliability, integrity and usability.

Emails are often regarded as an ephemeral form of communication. This misconception about how email can be used could result in legal action being taken against the FSA or individual staff.

You should treat emails in the same way as you would treat any other form of communication that can be recorded. You should type or write them as if someone else was looking over your shoulder.

The importance of this is emphasised by the fact that emails are subject to Data Protection and Freedom of Information legislation and can also form part of the corporate record. Staff should be aware that emails could be used as evidence in legal proceedings and may be released to the public in response to a FOIA request.

Items that are not records for example authorised personal emails as defined in the Employee Handbook, Section 11, Supplement 2, Annex 1 (<http://connect/fsahandbook/supplement/supplement1102.html>) should not be placed in FSA record keeping systems and should be disposed of as soon as possible.

It is the responsibility of all members of staff to manage their emails appropriately in order to comply with Data Protection and Freedom of Information legislation.

To manage emails appropriately staff must identify those which are records of their business activities and those which are ephemeral.

- Emails that might constitute a record are likely to contain information relating to business transactions that have or are going to take place, decisions taken in relation to the business transaction or any discussion that took place in relation to the transaction.
- Emails regarded as ephemeral contain no information relating to business transactions, for example arranging a date for a meeting, receipt for acceptance of a meeting.

It is important that emails that are identified as records are moved from personal email boxes (e.g. inbox, sent box or folders created under an inbox) and managed in the same way as other records. To prevent loss of valuable information, email messages must be acted upon and moved to the central storage area as quickly as possible.

Ephemeral emails should be managed within the individual's mailbox and kept for only as long as required before being deleted.

1.1 What is an 'authentic' record?

Description

An authentic record is one that can be proven to:

- a) be what it claims to be;
- b) have been created or sent by the person said to have created or sent it;
- c) have been created or sent at the time claimed;
- d) have not been tampered with; and

- e) be credible and authoritative so that evidence can be safely derived from it (for example to be used at FSA Tribunals, courts).

Standard

To ensure the authenticity of records, each Division should set up and document procedures that control the creation, receipt, transmission, maintenance and disposition of records. Each Division should also ensure that record creators are authorised and identified and that records are protected against unauthorised addition, deletion, alteration, use and concealment.

1.2 What is a 'reliable' record?

Description

A reliable record is one whose contents can be trusted as a full and accurate representation of the transactions, activities or facts they concern and can be depended on in subsequent transactions or activities.

Standard

Records should be created at the time of the transaction or activity to which they relate, or soon afterwards. They should be created by individuals who have direct knowledge of the facts or by systems routinely used within the business to complete a transaction or activity.

1.3 What is the 'integrity' of a record?

Description

The integrity of a record refers to its being complete and unaltered.

Standard

Records should be protected against unauthorised alteration. Divisional records management procedures should specify what additions or annotations may be made to a record after it is created, under what circumstances additions, or annotations may be authorised, and who is authorised to make them. Any authorised annotation, addition or deletion to a record should be explicitly indicated and traceable.

1.4 What makes a record 'useable'?

Description

A useable record is one that can be located, retrieved, presented and interpreted. It should be capable of subsequent presentation as directly connected to the business activity or transaction that produced it. The contextual linkages of records should carry the information needed for an understanding of the

transactions that created and used them. It should be possible to identify a record within the context of broader business activities and functions. The links between records that document a sequence of activities should be maintained.

Standard

Records should be arranged in a record keeping system in accordance with local procedures based on FSA's RMPS, that enables the FSA to obtain maximum benefit from quick and easy retrieval of information.

Types of registered file referencing systems include:

- alphabetical
- numerical
- alpha-numeric (FIN 14 / 1)
- keyword

The alpha-numeric system is most commonly used, as the letters can be used to indicate the function or business process that the files cover. The letters are often a prefix of the department the files originate from such as F or FIN to denote Finance Department, or PER to denote Personnel.

Irrespective of the type of filing system you choose it is essential that the system is simple and easily understood by users of the filing system and be capable of easy transfer e.g. in case of a business restructure.

For more information and guidance please contact John Newcombe in the Information and Records Management Team.

Electronic FSA records should be stored on the FSA central storage area and must be named in accordance with FSA naming conventions and principles for electronic record keeping.

NAME SUBJECT DATE (YYYYMMDD)

Please note the name should be the project or firm name and not the author's name

Examples

ADMINISTRATION

Dept A Meeting 20040505

FIRMS

Ahi United Bank Waiver 20040510

HANDBOOK

DEC 4.3 Executive procedures 20040510

Please note that you are not required to use underscores to separate each term; a space should be used to separate them.

All electronic records must be named in accordance with FSA naming conventions and principles for electronic record keeping.

2 How do I decide what is a record?

Description

To decide whether something is a record, look at it in the context of:

- the regulatory environment;
- business and accountability requirements; and
- the risk of not keeping it.

Standard

Items should be captured as records and linked with metadata which characterise:

- their specific business context when they commit someone to do something;
- give them responsibility for something; or
- record something that has happened.

Emails can constitute part of the formal record of transaction. All FSA staff are responsible for identifying and managing emails that constitute a record of their work.

When deciding whether an email constitutes a record, the context and content of the email needs to be considered.

Emails that might constitute a record are likely to contain information relating to business transactions that have or are going to take place, decisions taken in relation to the business transaction or any discussion that took place in relation to the transaction. If an email needs to be forwarded for information purposes it should be considered as a record.

As emails can be sent to multiple recipients the following guidelines should be followed to identify who is responsible for capturing an email as a record:

- For internal messages, the sender of an email, or initiator of an email dialogue that forms a string of emails
- For messages sent externally, the sender of the email
- For external messages received by one person, the recipient
- For external messages received by more than one person, the person responsible for the area of work relating to the message. If this is not clear then it may be necessary to clarify who this is

2.1 Version control

Description

Sometimes (for example during the development of policy) successive drafts of a document must be kept to provide adequate evidence of the process e.g. substantial changes during the development of policy.

Standard

The need to keep successive versions of items should be based on an analysis of record keeping requirements and should be documented in local procedures.

3 Why do we need to 'capture' records?

Description

Capturing a record means to place it in a records management system.

We need to capture items as records to:

- establish a relationship between the record, the creator and the business context that originated it (that is, why it was created);
- place the record and its relationship within a records system;
- link it to other records; and
- ensure that appropriate audit trails are maintained

To 'capture' a record, we need to allocate explicit metadata, embedded in, attached to or associated with the specific record, whatever its format.

This metadata is essential for accurately re-tracing the status, structure and integrity of the record at any particular time and showing its relationships with other records.

Techniques to ensure capture of records include:

- a) classification and indexing which allow appropriate linking, grouping, naming, security protection, user permissions and retrieval, disposition, and identifying vital records (see also Section 5);
- b) arrangement in a logical structure and sequence, whether a physical (paper) file or an electronic directory, which helps with further use and reference (see also Section 5);
- c) registration which provides evidence of the existence of records in a records system (see also Section 3.1); and
- d) systems that control the actions undertaken in doing business, which:

- i. provide metadata describing the business context;
- ii. provide evidence of where a record is located;
- iii. identify what action is outstanding;
- iv. identify who has accessed a record;
- v. identify when such access took place; and
- vi. provide evidence of the transactions that have been undertaken on the record (in other words an audit trail).

Standard

Items that have been identified as records must be captured in recognised FSA record keeping systems.

Emails that constitute records must be captured (saved) on the central storage area, in Message Format (*.msg) and put into folders with other records relating to the same business activity. The original email should be deleted from the personal mail box that it came from.

Where paper files are maintained, it may be more appropriate to place a copy of the email on that file. Local procedures should make that clear.

Emails will often form part of an email exchange string. Where this occurs it is not necessary to capture each new part of the exchange, i.e. every reply, separately.

You should not wait until the end of the conversation before capturing the email string as several subjects may have been covered. Email strings should be captured as records at significant points during the exchange, rather than waiting to the end of the exchange because it may not be apparent when the string has finished.

3.1 Why do we need to 'register' records?

Description

The main purpose of registration is to provide evidence that a record has been created or captured in a records system. It also helps in retrieving the record.

It involves recording brief descriptive information or metadata about the record, and assigning the record a unique identifier. Registration formalises the capture of the record into the records system.

In a records system that uses registration processes:

- a record is registered when it is captured into the records system (this may include placing a manual record into a structured filing system or the automated registration of electronic records in an electronic record keeping system); and

- no further processes affecting the record can take place until its registration is complete.

Records may be registered at more than one level (for example at the file series, file or record level) within a records system. In the electronic environment, records systems may be designed to register records automatically, in a way that is transparent to the user of the business system from which it is captured and without the need for a record manager.

Standard

The level at which a record needs to be registered, i.e. at the file or record level, should be decided by the need to provide evidence of its authenticity.

4 How long do I need to keep a record?

Description

You should decide how long to keep a record by assessing:

- the statutory and regulatory environment;
- business and accountability requirements; and
- the risks associated with keeping or disposing of the record at any particular point in time.

Statutory or other regulatory requirements (for example Data Protection) may demand that the record is kept for a minimum time or sent to an authorising body such as an archival authority or auditors for any necessary approval. You need to consider the rights and interests of all stakeholders when deciding how long records need to be maintained. The decisions should not be made to get round any rights of access.

Records identified for retention are likely to be those which:

- provide evidence and information about our policies and actions;
- provide evidence and information about our interaction with stakeholders;
- document the rights and obligations of individuals and organisations;
- contribute to the FSA's historical record; and
- contain evidence and information about activities of interest to internal and external stakeholders.

Standard

Records should be kept to:

- meet current and future business needs;
- comply with statutory, legal and corporate governance best practice requirements, by ensuring that the way we manage records is documented, understood and implemented; and
- reasonably meet the current and future needs of internal and external stakeholders.

Records that are no longer required should be eliminated as early as possible and in an authorised, systematic manner (see also section 9 below).

Divisions/Departments should create and maintain retention schedules. Retention schedules should state how long each record series should be kept and the justification for these periods.

The current FSA retention schedules are listed in Annex A of the RMPS or can be found on Connect http://connect/docs/RecordsMgt/retention_criteria.xls. If you require additions or changes to a schedule you must notify IRM.

Advice and guidance on retention and disposal best practice can be found in Annex B - Recommended Retention and Disposal Practices.

Line managers are responsible for ensuring their retention and disposal policy is maintained and implemented. Records authorised for disposal must be destroyed safely and securely, ensuring the information can not be reconstructed (see also section 9 below).

4.1 What is a 'vital record'?

Description

A vital record is one that is essential to the continued operation of the organisation following a disaster.

Standard

Vital records must be identified and protected to minimise the risk of loss if there is a disaster. This will form part of a contingency or business plan to provide protection for records vital to the continued functioning of the FSA. Protection can take the form of secure storage (for example in a fire resistant cabinet) or the maintenance of one or more backup copies which are stored in different locations, or both.

Under the FSA Business Continuity Plan each Division/department must ensure they have a Battlebox containing material that is critical to the successful initial recovery and functioning of the Division/department. (For more information on the FSA Business Continuity Plan policies and guidance please go to http://connect/fsa_services/business_continuity/policies_guidance.html)

5 What are subject classification and indexing? And why are they necessary?

Description

Subject classification of records, based on business activity, acts as a powerful tool to help us conduct our business and many of the processes involved in managing records, including:

- a) providing links between individual records we collect for a continuous record of activity;
- b) making sure records are named consistently over time;
- c) helping in the retrieval of all records about a particular function or activity;
- d) deciding security protection and appropriate access for sets of records;
- e) allocating user permissions for access to or action on particular groups of records;
- f) distributing responsibility for management of particular sets of records;
- g) distributing records for action; and
- h) deciding appropriate retention periods and disposition actions for records.

Standard

Metadata describing the subject content should be linked with records at the appropriate level (i.e. file series, file or record level) to meet the anticipated retrieval needs.

5.1 What is a subject classification system?

Description

Subject classification is based on an analysis of the FSA's business activities. These systems can be used to support various records management processes.

5.2 What is an index?

Description

An index gives the user an efficient means of tracing information. An index or indices should allow the user to:

- a) understand it easily, enabling them (and their successors) to quickly establish the presence or absence of information on a given subject;
- b) identify and locate relevant information within records;
- c) group together information on subjects; and
- d) search for information using indexing terms that are appropriate to their needs.

Indexing can be done manually or be automatically generated. It may occur at various levels of aggregation (file series, file or record level) within a records system and includes full text indexing.

5.3 What is vocabulary control?

Description

A vocabulary control is an agreed list of keywords or terms which are used for specific purposes, for example a thesaurus.

Vocabulary controls should explain organisation-specific definitions, abbreviations or usage of terms. Subject classification systems and indexes may be supported by vocabulary controls that are suited to the complexity of the records of an organisation.

5.4 Why use numbers and codes as well as using titles?

Description

Shorthand methods of referencing records by means other than the title are commonly used. Allocating numbers or codes to a group (file series, file or record level) of records is quite common. Coding records can help locate them where the number or code indicates the 'address' of the record and so may also be used to retrieve the record.

6 How do I store and handle records?

Description

You need to consider the specific physical properties of records to decide how to store and handle them. Records that continue to be useful and relevant, no

matter what format they are in, need appropriate storage and handling to preserve them for as long as they are needed.

Standards

Storage conditions and handling processes should be designed to protect records from unauthorised access, loss or destruction, and from theft and disaster.

Records should be stored on media that ensure their usability, reliability, authenticity and preservation for as long as they are needed (see also Section 4.1 above).

Issues relating to the maintenance, handling and storage of records arise throughout their existence.

Systems for electronic records should be designed so that records are accessible, authentic, reliable and useable through any kind of system change, for as long as they are kept. This may include transfer to different software, formats or any other future ways of re-presenting records. Where such processes occur, evidence of these should be kept, along with details of any variation in records design and format.

7 Access and security of stored records

Description

The regulatory environment in which we operate sets the broad principles on access rights, conditions or restrictions that should be incorporated into the records systems. These should consider legislation covering areas such as privacy, data protection, security, and freedom of information. Records may contain personal, commercial or operationally sensitive information. In some cases access to the records, or information about them, should be restricted.

Restrictions on access can be applied both within the organisation and to external users, and should reflect the legal and other rights of the FSA, its stakeholders and any other persons affected by its actions.

Restricted records should be identified as such, only where specifically required by a business need or the regulatory environment. *Restrictions should be imposed for a stated period, to ensure that the additional monitoring required for these records is not enforced for longer than needed.*

The need to place restrictions on accessibility can change with time; but it should be noted that adding a restriction to a record does not necessarily prevent access to the record or the information. The Freedom of Information Act³ is intended to promote a culture of openness and accountability amongst public authorities. It promotes disclosure of information, unless an exemption applies and even then a public interest test may be applied.

3 The Freedom of Information Act 2000 came fully into force on 1st January 2005

The use and application of restrictions to FSA records should be carefully considered as requests for information made under the Data Protection Act and the Freedom of Information Act could still result in the information having to be released, irrespective of any restrictions previously applied.

Ensuring appropriate access controls is done by assigning access status to both records and individuals.

Managing the access process involves ensuring that:

- a) records are categorised according to their access status at a particular time;
- b) records are only released to those who are authorised to see them;
- c) encrypted records can be read as and when required and authorised;
- d) records processes and transactions are only undertaken by those authorised to perform them; and
- e) parts of the organisation with responsibility for particular business functions specify access permissions to records relating to their area of responsibility.

The monitoring and mapping of user permissions and functional job responsibilities is a continuing process, which occurs in all records systems regardless of format.

Standards

Local records management policies should include guidelines, regulating who is allowed access to records and in what circumstances. The FSA's standard security markings should be adopted. See Part F – Security Markings.

Whitehall documents must be managed in line with the appropriate procedures.

All FSA staff should be aware of their responsibilities for compliance with security procedures for electronic records.

All FSA staff should understand:

- that FSA records are unrestricted unless access restrictions have been explicitly requested and put in place;
- the circumstances where FSA records should be restricted taking into account the FSA's obligations under the Freedom of Information Act ;
- the process for having restrictions added or removed from FSA records;
- their responsibilities for handling highly market sensitive information (HMSI documents/information have restricted access for a specified time period, that is specified at the time of applying the restriction and a date is set to review the removal of the restriction);

- their responsibilities under the Data Protection Act for handling records about named individuals;
- their contractual duties relating to confidential information;
- how to protect records using security markings;
- the process for restricting access to records where a crisis occurs within a firm.

8 Why do I need to keep track of records?

Description

Tracking of the movement, location and use of records within a records system is required to:

- a) identify outstanding action required;
- b) enable retrieval of a record (to include the ability to track records stored in different media, for example electronic and hard copy);
- c) prevent loss of records;
- d) monitor use of systems maintenance and security, and maintain an auditable trail of records transactions (that is, capture or registration, classification, indexing, storage, access and use, migration, transfer or disposal); and
- e) maintain the ability to identify the origins of individual records where systems have been amalgamated or migrated.

8.1 When should I use 'action tracking'?

Description

Action tracking may be used in a records system where time limits for actions are imposed by or on the organisation. Action tracking:

- a) allocates steps to be taken in response to decisions or transactions documented in a record;
- b) assigns responsibility for action to a designated person; and
- c) records dates by which the predefined action is to be taken and dates when those actions occur.

Action tracking can only be effectively used if material is registered into the records system before forwarding to the designated persons.

8.2 Why do I need to keep track of a record's location?

Description

The movement of records should be documented to ensure that items can always be found when required.

Tracking mechanisms may record the item identifier, the title, the person or unit possessing the item and the time/date of movement.

Standard

To provide an audit trail, the system should track the issue, transfer between persons, and return of records to their 'home' location or storage. The system should also track their disposition or transfer between Divisions/Departments and authorised external organisations including external stores or archives.

9 When and how do we dispose of records?

Description

Disposition is the process of deciding whether to keep, move or destroy records. This process is governed by disposition authorities (or retention schedules).

These govern the removal of records from operational systems and they should be used on a systematic and routine basis. No 'disposition action' should take place without the assurance that:

- the record is no longer required;
- no work is outstanding; and
- no litigation, investigation or access request is current or pending which is relying on that record.

'Disposition action' is the:

- a) immediate physical destruction, including overwriting and deletion;
- b) retention for a further period within the business unit;
- c) transfer to an appropriate storage area or medium under Divisional/Departmental control;
- d) transfer to another organisation that has assumed responsibility for the business activity through restructure, sale or privatisation;
- e) transfer to a storage area managed for the FSA by an external provider where appropriate contractual arrangements have been entered into;

- f) transfer of responsibility for management to an appropriate authority while physical storage of the record is kept by the creating organisation; or the
- g) transfer of records to an external archive, for example the Bank of England or The National Archive.

Standards

Local records management policies must include retention schedules that clearly state the retention period of each type of record captured by the business unit. The date the retention periods starts should be clear and procedures and system(s) should be put in place to ensure records are reviewed on a specified review date.

Through the review process records should be:

- Retained for a further specified period
- Transferred to The National Archives if records are selected for permanent preservation
- Destroyed

Destruction must always be authorised. The records should only be destroyed by authorised staff in accordance with the business unit's retention and disposal schedules.

Records relevant to pending or actual litigation, investigation or access requests must not be destroyed.

Authorised records destruction should be carried out in a way that preserves the confidentiality of any information they contain.

All copies that are authorised for destruction, including security copies, preservation copies and backup copies, should be destroyed.

A record should be held of which items have been eliminated/destroyed (disposal schedule), together with the appropriate authorisations.

For more information and advice on records management please go to Connect <http://connect/fsa/RSS/RTS/P&I/PIInfoAccess.html#recordsmgmt> or contact the Information and Records Management Team - RM specialist, John Newcombe ext. 60744 or by email.

D Glossary of terms

Access

Right, opportunity, means of finding, using or retrieving information. [ISO 15489]

Accountability

Principle that individuals, organisations, and the community are responsible for their actions and may be required to explain them to others. [ISO 15489]

Action tracking

Process in which time limits for actions are monitored and imposed on those conducting the business. [ISO 15489]

Classification

Systematic identification and arrangement of business activities and/or records into categories according to logically structured conventions, methods, and procedural rules represented in a classification system. [ISO 15489] See also Security Marking

Conversion

Process of changing records from one medium to another or from one format to another. [ISO 15489]

Destruction

Process of eliminating or deleting records, beyond any possible reconstruction. [ISO 15489]

Disposition (keeping, moving or removing records)

Range of processes associated with deciding whether to keep, destroy, or transfer records. These are documented in disposition authorities, retention schedules or other instruments. [ISO 15489]

Document, noun

Recorded information or object which can be treated as a unit. [ISO 15489]

Indexing

Process of creating access points to facilitate retrieval of records and/or information. [ISO 15489]

Metadata

Data describing context, content and structure of records and their management through time. [ISO 15489]

Migration

Process of moving records from one system to another, while maintaining the records' authenticity, integrity, reliability and usability. [ISO 15489]

Preservation

Processes and operations involved in ensuring the technical and intellectual survival of authentic records through time. [ISO 15489]

Record series

A group of related records that are normally used and filed together or otherwise linked and that allow consideration as a unit for use, review, retention or destruction purposes.

Records

Information created, received and maintained as evidence and/or information by an organisation or person, in pursuance of legal obligations or in the transaction of business. [ISO 15489]

Records management

Field of management responsible for the efficient and systematic control of the creation receipt, maintenance, retrieval, use and disposition of records. These include processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records. [Based on ISO 15489]

Registration

Act of giving a record a unique identifier on its entry into a system. [ISO 15489]

Retention schedule

See Disposition

Security marking

Indicators defining the handling, storage and disposal arrangements, which are required to protect the material to a level appropriate to its sensitivity.

Tracking

Creating, capturing and maintaining information about the movement and use of records. [ISO 15489]

Transfer [custody]

Change of custody, ownership and/or responsibility for records. [ISO 15489]

Transfer [movement]

Moving records from one location to another. [ISO 15489]

Vital records

Records, in whatever form, that are essential to the continued operation of the FSA after a disaster (business recovery).

E References and links

British Standards Institution (BSI). *Information and documentation – guidelines for the content, organization and presentation of indexes*. BS ISO 999:1996

British Standards Institution (BSI). *Information security management*. BS 7799 parts 1 and 2:1999

British Standards Institution (BSI). *Recommendations for examining documents, determining their subjects and selecting indexing terms*. BS 6529:1984

Financial Services Authority (FSA). *FSA IS Information Security Manual*, version 0.4, October 2002.
<http://connect/docs/is/IS%20Information%20Security%20Manual%20v0.4.pdf>

International Organization for Standardization (ISO). *Information and Documentation – Records management*. ISO 15489 2000

International Organization for Standardization (ISO). *Information and Documentation – Documentation storage requirements for archive and library materials*. ISO/IEC DIS 11799

Lord Chancellor's Department. *Code of Practice on the Management of Records Under Freedom of Information*. Stationery Office, London, June 2000.
<http://www.dca.gov.uk/foi/codemanrec.htm#part8>

The National Archives. Guidelines on developing a policy for managing email. 2004
http://www.nationalarchives.gov.uk/electronicrecords/advice/pdf/managing_emails.pdf

The National Archives – Records Management Advice, Retention and Disposal schedules – Retention Scheduling 11. Internal Audit Records
http://www.nationalarchives.gov.uk/recordsmanagement/advice/pdf/sched_internal_audit.pdf

The National Archives – Records Management Advice, Retention and Disposal schedules – Retention Scheduling 4. Health and Safety Records
http://www.nationalarchives.gov.uk/recordsmanagement/advice/pdf/sched_health_safety.pdf

The National Archives – Records Management Advice, Retention and Disposal schedules – Records Management: Retention Scheduling 5. Contractual Records
http://www.nationalarchives.gov.uk/recordsmanagement/advice/pdf/sched_contractual.pdf

The National Archives – Records Management Advice, Retention and Disposal schedules – Records Management: Retention Scheduling 8. Press and Public Relations Records. Version 1, March 2002
http://www.nationalarchives.gov.uk/recordsmanagement/advice/pdf/sched_press.pdf

F Security Markings

The term 'security marking' is used in order to differentiate between these markings and 'protective markings' used by central Government.

The security marking system is used to ensure that assets for which the FSA is responsible are protected against compromise, including loss, theft, disclosure, destruction and tampering.

Definitions

There are four levels of security marking. Each level defines the handling, storage and disposal arrangements, which are required to protect the material to a level appropriate to its sensitivity. In addition to a security marking, records may also be given a Handling Descriptor which gives the FSA recipient or handler, information about how to deal with that particular record. These handling descriptors are set out in Table 4 below.

Table 1: Definitions of Security Markings

FSA Marking	FSA Interests	International Relations	Economic Interests	Law Enforcement
	If compromised, this material would be likely to:			
FSA Top Secret	Cause exceptionally grave damage to the FSA or jeopardise our ability to fulfil many of our key objectives, or pose a risk to the life of FSA staff or others	Cause exceptionally grave damage to relations with friendly governments. Threaten directly the internal stability of friendly countries.	Cause severe long-term damage to the UK economy.	
FSA Secret	Cause serious injury to the FSA's long-term interests and confidence in the FSA (e.g. through the loss of highly sensitive information passed to us by another regulator).	Raise international tension. Damage seriously relations with friendly governments.	Cause substantial material damage to national economic and commercial interests.	
FSA Restricted	Be damaging to the FSA's interests (e.g. through mislaying confidential papers passed to us by a third party or revealing FSA's position)	Affect adversely diplomatic relations.	Cause financial loss or loss of earning potential to or facilitate improper gain or advantage for individuals or companies.	Prejudice the investigation of crime. Facilitate the commission of crime.
FSA Unrestricted	May be disclosed without damage to any interests			

Table 2: Creation and Handling Requirement

Action	Unrestricted	FSA Restricted
Preparation: Marking	Use FSA 'unrestricted' versions of templates. (To be developed for Word, Excel, PowerPoint)	No special requirements – use FSA 'restricted versions of templates1
Preparation: Numbering of copies	Not required	
Registration (Logging)	<p>Material received from an external (non-FSA) source: Divisional logging procedures must be followed. If the document is to be retained as a record it must be registered and a decision taken on whether to apply a higher security marking or Handling Descriptor [e.g. HMSI]</p> <p>For internal correspondence, Divisional logging procedures must be followed. If the document is to be retained as a record it must be registered.</p>	
Copying	No restriction	
Circulating Records within FSA	Not restricted	No restriction unless Handling Descriptor applied
Disclosing Records outside FSA (when permitted) by legislative gateways, confidentiality etc)	Not restricted	Not permitted except with specific consent and subject to legislative gateways: (as the classification 'FSA RESTRICTED' implies, this material is restricted to the FSA only)
Removing Records from FSA premises (when permitted)	Not restricted	Can be removed for off-site working, meetings or working at home (but not in public, e.g. on public transport). Should be locked away when not in use. Should not be the only copy and any file/Record movements must be recorded
Movement of Physical Items Within an FSA Building (including to/from filing)	Not restricted	Restricted to FSA employees and those who have signed a confidentiality agreement. Original Records and files should only be lent out in accordance with local guidelines; Recipient areas are responsible for all files and Records lent to them from other areas
Movement of Physical Items Between FSA Buildings	Not restricted	<p>Restricted to FSA employees who have been subject to all Basic Recruitment checks and who have signed a confidentiality agreement. Originals (Records and files) should only be lent out in accordance with local procedures and all file/Record movements away from the 'local' area must be tracked</p> <p>Use sealed envelope marked 'FSA RESTRICTED'</p>

Action	Unrestricted	FSA Restricted
Facsimile Transmission	Use FSA Fax cover sheet template.	Use FSA Fax cover sheet template, which includes Confidentiality Note
Internal Electronic Mail transmission (within FSA)	Not restricted	Follow FSA E-mail Guidelines http://connect/info/policies/is/email_guidelines_a.html
External Electronic Mail transmission (via the Internet –when permitted)	FSA ‘signature’ and confidentiality statement automatically added to emails.	Follow FSA E-mail Guidelines http://connect/info/policies/is/email_guidelines_a.html FSA ‘signature’ and confidentiality statement automatically added to emails
FSA Shared Drives (including Tracker tools)	Not restricted	Follow Divisional procedures subject to any Handling Descriptor
Review of Security Marking	Not necessary	Follow Divisional procedures
Destruction Authorisation	See Records Management Standards and Policy	
Destruction of Physical Records	Follow Divisional procedures	Follow Divisional procedures Use Confidential Waste disposal
Destruction/Deletion of Electronic Records	Follow Divisional procedures and IS guidance	Follow Divisional procedures and IS guidance

Table 3: Handling and Protecting Secret and Top Secret Information

Activity	Secret	Top Secret
Creating a new document	Use stand-alone PC only. Do not use e-mail or networked printers.	
Saving a document	May be saved on disc and disc held as secret record	May be saved on disc and disc held as Top Secret record
Registration	All Secret records should be registered in a log maintained by the individual in each Division responsible for controlling Secret Records	All Top Secret Records should be registered in a log maintained by the Whitehall Documents team
Storage	All Secret records should be stored in secure cabinets meeting standards specified by Whitehall Documents team and under the control of the individual responsible for these records in each Division	All Top Secret records should be stored in secure cabinets under the control of the Whitehall Documents team

Activity	Secret	Top Secret
Material from outside FSA	Immediately on determination of Secret status of record incoming material should be registered and come under the control of the individual responsible for these records in each Division	Immediately on determination of Top Secret status of record, incoming material should be registered with Whitehall Documents team and controlled by them. Copies must be number and allocated to specified recipients and stored as Top Secret records by all recipients
Copying	Copies should only be produced by staff with authorised access to the information. Copy only if no restriction specifically mentioned in the text of the document. Copies must be number and allocated to specified recipients and stored as Secret records by all recipients	Should not be copied unless absolutely necessary. Copies should only be produced by staff with authorised access to the information. Copy only if no restriction specifically mentioned in the text of the document
Circulating documents within FSA	Use double new envelopes. Flaps sealed with tape and initialled. Marking or classification on inner envelope only. Address to specific individual.	
Disclosing documents outside FSA	Double new envelopes. Flaps sealed with tape and initialled. High security tape on inner envelope for Government material. Marking or classification on inner envelope only. Address to specific individual or job title. Use FSA contracted courier. Documents addressed to external recipients should be entered on computer log and allocated unique number. Individual document receipts only required for Secret documents sent outside FSA where authorised courier not used	Double new envelopes. Flaps sealed with tape and initialled. High security tape on inner envelope for Government material. Marking or classification on inner envelope only. Address to specific individual or job title. Use authorised courier. Documents addressed to external recipients should be entered on computer log and allocated unique number. Individual document receipts required for all Top Secret documents sent outside FSA
Removing documents from FSA premises	Only remove (in briefcases with double lock and robust enough to withstand being dropped without opening) on single occasions, i.e. for a meeting, if absolutely necessary. Must not be the only copy. Should not be taken home unless suitable container available to store it. Permission required from HoD. Must be written down and known to all relevant staff	Only remove (in briefcases with double lock and robust enough to withstand being dropped without opening) on single occasions, i.e. for a meeting, if absolutely necessary. Must not be the only copy. Should not be taken home unless suitable container available to store it. Permission required from HoD. Authority given specifically to individuals authorised to see content. Authority must be written down and known to all relevant staff

Activity	Secret	Top Secret
Movement of physical items within FSA	Individual documents should not be lent out of files unless absolutely unavoidable. If lent out they should be entered on the log	
Fax	Use only secure fax machine over a direct link to the institution concerned. Telephone receiving end to ensure receiving terminal manned by someone authorised to see the material. Ensure no unauthorised person in position to overlook terminal during transmission. Transmission and receipt of each item marked Secret should be recorded in log-books associated with the terminals	Use only secure fax machine over a direct link to the institution concerned. Telephone receiving end to ensure receiving terminal manned by someone authorised to see the material. Ensure no unauthorised person in position to overlook terminal during transmission. Transmission and receipt of each item marked Top Secret should be recorded in log-books associated with the terminals
Internal emails (within FSA)	Do not use e-mail	
External emails (outside FSA)	Do not use e-mail	
FSA shared drives (access)	Do not use shard drives	
Review of security markings	Originator or Divisional Director	Originator or Company Secretary via Whitehall Documents
Authorising destruction	Originator or initial recipient plus Divisional Director	Originator or initial recipient plus Company Secretary via Whitehall Documents
Destruction of physical documents	Cross cut shredder or appropriate waste sacks. Disposal should be recorded on log. Initials of person destroying document and date of destruction should also be noted on log	Cross cut shredder or appropriate waste sacks. Disposal of individual documents should be recorded on log. Initials of person destroying document and date of destruction should also be noted on log
Destruction/deletion of electronic records	Erase or destroy discs	

Table 4: FSA-Wide Handling Descriptors

Descriptor	Purpose
Addressee(s) only	For material to be seen only by the addressees in the first instance. Divisions' procedures for handling incoming material from other FSA Divisions must ensure that items marked 'Addressee Only' are delivered to and seen only by the named addressees. The originator may use email at their discretion but must recognise that doing so may mean that others sharing access to an addressee's 'Inbox' may also see the message. If circulating in hardcopy, documents should be put in a sealed envelope marked as "Addressee only". "Addressee only" marked records should not be circulated to others without the originator's agreement. Subsequent storage in electronic or hard copy form should reflect the sensitivity of the content. That may mean storage in a personal record series for a period but ultimately these records should be incorporated into Division/Departmental filing and managed accordingly.
Board	To identify papers prepared for the FSA's Board or its members. To be handled in accordance with local procedures for maintaining the confidentiality of those records appropriate to their content.
HMG Confidential	To identify HMG view of sensitivity of material contained in (or attached to) a record. No special handling requirements. (See Directorates/Operations/HR section on Connect under 'line managers guidelines).
Highly Market Sensitive Information	To restrict access to information which is particularly market sensitive. Please note that information deemed Highly Market Sensitive Information will have restricted access applied for a specified time period. The time period must be indicated at the point when HMSI is applied and should be reviewed periodically.
Legal privilege	To identify status. No special handling requirements.
Staff	To indicate that records should be kept only in accordance with HR guidance on staff matters.

FSA Retention Schedules

FSA Retention criteria for Supervisory/Regulatory Records

<u>Supervision Records</u>	<u>Known Best Practice</u>	<u>Operational Requirements</u>	<u>Legal requirements</u>
Records transferred, presented or loaned to FSA by former constituent bodies prior to N2			
Supervisory records transferred to FSA from the Bank of England (BoE) 1979 to 1998	The Bank of England to have permanent right of access to S&S records post 1979 transferred to FSA, retaining legal liability for supervisory decisions taken prior to transfer. (Ref. BoE note November 1997)	Return to Bank of England after 7 years for destruction or inclusion in the Bank's archive.	
Regulatory records of former constituent bodies SIB ¹ , PIA ² , SFA ³ , IMRO ⁴ , LAUTRO ⁵ , FIMBRA ⁶ .		Destroy after 7 years	
SIB ¹ , PIA ² , SFA ³ , IMRO ⁴ , LAUTRO ⁵ , FIMBRA ⁶ , TSA ⁷ , IBRC ⁸ , AFB ⁹ , DTI ¹⁰ , Bank of England's S&S, INS Dir, Friendly Soc. Commission Legacy information on rule books, publications, press releases and disciplinary details only (public and private)		Permanent retention	

¹ Securities and Investment Board

² Personal Investment Authority

³ Securities and Futures Authority

⁴ Investment Management and Regulatory Authority

⁵ Life Assurance and Unit Trust Regulatory Organisation Limited

⁶ Financial Intermediaries, Managers and Brokers Regulatory Association

⁷ The Securities Association

⁸ Insurance Brokers Registration Council

⁹ Association of Futures Brokers & Dealers

¹⁰ Department of Trade and Industry

Version 1.3

October 2004

Financial Services Authority 2004-2005

FSA Retention criteria for Supervisory/Regulatory Records

<u>Supervision Records</u>	<u>Known Best Practice</u>	<u>Operational Requirements</u>	<u>Legal requirements</u>
<p>Pre N2 records held by FSA on behalf of predecessor bodies under HMG</p> <ul style="list-style-type: none"> i) Building Societies Commission ii) Friendly Societies Commission iii) HMT and DTI documents relating to Insurance regulation between 01/01/1999 to 01/12/2001 <p>Mutual Societies records for public access</p>	<p>National Archives guidance – documents selected for permanent preservation should be transferred to National Archives within 30 years of selection</p> <p>National Archives guidance – documents selected for permanent preservation should be transferred to National Archives within 30 years of selection</p> <p>National Archives guidance – documents selected for permanent preservation should be transferred to National Archives within 30 years of selection</p>	<p>Destroy after 7 years unless selected for preservation by the National Archive</p> <p>Destroy 7 years after the closure of the society</p> <p>Destroy 10 years after the advice was given unless selected for preservation by the National Archives (Government Actuary – retention of documents 9 September 1997)</p>	
<p>Pre N2 records held by FSA on behalf of Government Actuaries Division</p>			

FSA Supervisory records from N2			
<u>Supervision Records</u>	<u>Known Best Practice</u>	<u>Operational Requirements</u>	<u>Legal requirements</u>
Supervisory records	Financial Services and Markets Act schedule 1 paragraph 9 and to meet the needs of HMT review	Destroy 7 years after year of creation unless rationale in business terms provided for specified records. Maximum retention 15 years	
Mutual Societies records for public access	Financial Services and Markets Act schedule 1 paragraph 9 and to meet the needs of HMT review	Destroy 7 years after closure of the society	
FSA retention criteria for Regulatory Process records			
<u>Regulatory Process Records</u>	<u>Known Best Practice</u>	<u>Operational Requirements</u>	<u>Legal requirements</u>
<u>Authorisation</u>			
Corporate	FSMA Schedule 1 paragraph 9 and to meet the needs of HMT review	Destroy 7 years	
Individual	FSMA Schedule 1 paragraph 9 and to meet the needs of HMT review	Destroy 7 years	
Approved Person regime-forms			
Form A application to perform controlled function		Destroy 10 years from date of receipt	
Form B notice to withdraw an application		Destroy 7 years	
Form C notice of ceasing to perform controlled functions		Destroy 10 years from date of receipt	
Form D notification of changes in personal information		Destroy 7 years	
Form E application for internal transfer of an approved person		Destroy 7 years	
<u>Enforcement</u>			
Enforcement action	FSMA Schedule 1 paragraph 9 and to meet the needs of HMT review	Destroy after duration of project plus 7 years	

FSA retention criteria for Regulatory records			
<u>Regulatory Process Records</u>	<u>Known Best Practice</u>	<u>Operational Requirements</u>	<u>Legal requirements</u>
Enforcement continued			
Seized evidence		[Return to owner] within 3 months, or if proceedings are commenced within that period, until the conclusion of proceedings	3 months, or if proceedings are commenced within that period, until the conclusion of proceedings
Intelligence gathering			
Research in support of FSA action	FSMA Schedule 1 paragraph 9 and to meet the needs of HMT review	Destroy after case closure plus 7 years unless rationale in business terms provided for specific records. Maximum retention is 15 years	
Risk Assessment	FSMA Schedule 1 paragraph 9 and to meet the needs of HMT review	Destroy 7 years after year of creation unless rationale in business terms provided for specific records. Maximum retention is 15 years	
FSA retention criteria for Legal records			
<u>Legal Records</u>	<u>Known Best Practice</u>	<u>Operational Requirements</u>	<u>Legal requirements</u>
Legal advice received (External legal opinion included in applications to FSA, e.g. in variation of permission requests, should be treated as information received and not as legal advice)	Limitations 6 years	Destroy after duration of action for which advice received plus 7 years	
Legal advice given	Limitations 6 years	Destroy after duration of action for which advice given plus 7 years	
Contract, agreements etc			
Contracts/agreements under seal		Destroy 12 years after conclusion of contract	Limitations Act 1980 12 year limit for actions on a contract under seal (i.e. companies memorandum)

FSA retention criteria for Legal records			
<u>Legal Records</u>	<u>Known Best Practice</u>	<u>Operational Requirements</u>	<u>Legal requirements</u>
<u>Contract, agreements continued</u>			
Other contracts		Destroy 6 years after conclusion of contract	6 years after expiry
Title deeds and property related documents		Destroy 12 years after expiry	[12 years after expiry ceased]
Major agreements		Permanent retention for lifetime of organisation	
Royalty payments		Permanent retention for lifetime of organisation	
Royalty agreements		1 year after expiry	1 year after expiry
<u>FSA retention criteria for Policy records</u>			
<u>Policy Records</u>	<u>Known Best Practice</u>	<u>Operational Requirements</u>	<u>Legal requirements</u>
Policy records	FSMA Schedule 1 paragraph 9 and to meet the needs of HMT review	Destroy 7 years after creation unless rationale in business terms provided for specific records. Maximum retention 15 years	
FSA rule books, publications, press releases and disciplinary details only (public and private) in both paper and electronic format including: FSA consultation papers, responses to consultation papers, FSA discussion papers and responses to discussion papers	FSMA Schedule 1 paragraph 9 and to meet the needs of HMT review	Permanent retention	

FSA retention criteria for Cross FSA records			
<u>Cross FSA Records</u>	<u>Known Best Practice</u>	<u>Operational Requirements</u>	<u>Legal requirements</u>
<u>Regulatory decision making</u> ChairCo Delegations	3 months for challenges under FSMA	Destroy 7 years after the version superseded.	6 years from date of loss for claims of negligence, with a Statutory limitation period of 15 years. 3 months for judicial review.
Agendas approved minutes and supporting internal and external papers.	3 months for challenges under FSMA	Destroy 7 years after the month in which the decision was made.	6 years from date of loss for claims of negligence, with a Statutory limitation period of 15 years. 3 months for judicial review.
Management information	3 months for challenges under FSMA	Destroy 2 years after the 31st March following the month to which the MI relates	6 years from date of loss for claims of negligence, with a Statutory limitation period of 15 years. 3 months for judicial review.
Statement of procedures for each Decision Making Committee	3 months for challenges under FSMA	Destroy 7 years after the version superseded	6 years from date of loss for claims of negligence, with a Statutory limitation period of 15 years. 3 months for judicial review.
Divisional regulatory committee (DRC) decisions	3 months for challenges under FSMA	Destroy 15 years from the date the final statutory notice was issued.	6 years from date of loss for claims of negligence, with a Statutory limitation period of 15 years. 3 months for judicial review.
Tribunal referrals	3 months for challenges under FSMA	Destroy 15 years from the date the final statutory notice was issued.	6 years from date of loss for claims of negligence, with a Statutory limitation period of 15 years. 3 months for judicial review.
FSA project work			
Project records		Project records destroy 7 years from completion of project	
Working papers		Draft reports, working papers & correspondence destroy 2 years from completion of project	

FSA retention criteria for Cross FSA records			
<u>Cross FSA Records</u>	<u>Known Best Practice</u>	<u>Operational Requirements</u>	<u>Legal requirements</u>
<u>Code of Conduct documentation</u>			
Appendix A Disclosure of interests		Retain 7 years from date of signing. All versions of Appendix As (including those copied to HR) should be retained from date of signing, even if they have been superseded by a revised version incorporating changes.	
Appendix B Permission to deal		Retain 7 years from date of signing (ideally in electronic form)	
Appendix C Compliance with the code		Hard copy original to be retained on HR's files. Retention as for personnel records 6 years from end of employment.	
<u>FSA retention criteria for HR records</u>			
<u>Central HR records - retention periods specified by HR data protection project</u>			
Wages /salary records (also overtime, bonuses, expenses)		Destroy 6 years	Review/destroy 6 years
Income tax & NI returns, income tax records, payroll & wages details.		Destroy not less than 6 years after the end of the financial year to which they relate	Review/destroy not less than 6 years after the end of the financial year to which they relate
Statutory sick pay records, calculations, certificates & self certificates.		Destroy not less than 3 years after the end of the financial year to which they relate	Review/destroy not less than 3 years after the end of the financial year to which they relate
Statutory maternity pay records, calculations, certificates (Mat B1s or other medical evidence).		Destroy not less than 3 years after the end of the financial year to which they relate	Review/destroy not less than 3 years after the end of the financial year to which they relate
<u>Records during employment</u>			
Application forms, interview notes and reference details.	Recommended retention period - HR Data Protection guidelines 2001	Retain for duration of employment.	

FSA retention criteria for HR records			
HR Records	Known Best Practice	Operational Requirements	Legal requirements
Records during employment continued			
Disciplinary details.	Recommended retention period – HR Data Protection guidelines 2001	Disciplinary details should be returned to HR for retention until the disciplinary action has expired. At expiry, the details will be destroyed. In any event disciplinary details should be removed one year after employment has ended.	
Sickness record	Recommended retention period – HR Data Protection guidelines 2001	Destroy 3 years	
Annual leave records	Recommended retention period – HR Data Protection guidelines 2001	Destroy 2 years	
Unpaid leave/special leave records	Recommended retention period – HR Data Protection guidelines 2001	Destroy 3 years	
Annual appraisal/assessment records	Recommended retention period – HR Data Protection guidelines 2001	Destroy 5 years	
Records retained after employment			
Personnel file and training records	Recommended retention period – HR Data Protection guidelines 2001	Destroy 6 years	
References given/information to enable references to be provided.	Recommended retention period – HR Data Protection guidelines 2001	Destroy 5 years from reference received/end of employment.	
Summary of record or service e.g. name, position held, dates of employment.	Recommended retention period – HR Data Protection guidelines 2001	Destroy 10 years from end of employment.	
Records relating to accident or injury at work.	Recommended retention period – HR Data Protection guidelines 2001	Review/destroy 12 years.	

FSA retention criteria for Financial records			
Financial Records	Known Best Practice	Operational Requirements	Legal requirements
Financial Records			
Accounting records		Destroy 3 years from date created	Companies Act 1985 s.222(5) accounting records retained 3 years from date made
VAT		Destroy 3 years from date created	Retain 3 years
Taxation		Review/destroy 6 years. Retained records for which rationale in business terms provided destroy at 15 years	Taxation Management Act 1970 retain 6 years NB s.39 TMA 1970 Inland revenue may investigate matters more than 15 years in exceptional circumstances
Cheques/remittance advice		Destroy 6 years	6 years
Cash book list		Destroy 10 years	10 years
Cost control ledger analysis		Destroy 6 years	6 years
Invoices			
Invoice – revenue	6 years		Destroy 6 years
Invoice – capital		10 years	Destroy 10 years
Quotations			
Capital expenditure (successful)		Permanent for lifetime of company	
Capital expenditure (unsuccessful)		Retain 1 year	
Revenue expenditure (successful)		Retain current plus 1 year	
Revenue expenditure (unsuccessful)		Retain 3 months	
Purchase requisitions	Current plus 3 years	Current plus 3 years	
Assets			
Ledger sheets	10 years		
Consolidated accounts		Permanent for lifetime of company	
Disposal of assets		Permanent for lifetime of company	
Application to write off plant value		Permanent for lifetime of company	
Annual depreciation		Retain 3 years	

FSA retention criteria for Corporate records			
Corporate Records	Known Best Practice	Operational Requirements	Legal requirements
Minutes of Committees or Board meetings		Permanent retention	Companies Act 1985
Directors minutes signed by the Chairman		Permanent retention	Companies Act 1985
Company registers		Permanent retention	Companies Act 1985
Powers of attorney & court orders		Permanent retention	Companies Act 1985
Copy of instruments creating change		Permanent retention	Companies Act 1986
Enquiry proceedings	Commercial	Permanent retention	
Company organisation papers	Commercial	Permanent retention	
Important company policy records	Commercial	Permanent retention	
Legal documents	Commercial	Permanent retention	
Register of seals		Permanent retention	Companies Act 1985
Articles of association		Permanent retention	Companies Act 1985
Certificate of incorporation		Permanent retention	Companies Act 1985
Register of directors and secretaries		Permanent retention	Companies Act 1985 s.288
Register of directors share and debenture interests		Permanent retention	Companies Act 1984 s.325
Particulars of directors service contracts		Permanent retention	Companies Act 1984 s.318
Contracts - see under Legal			
FSA retention criteria for Administrative records			
Administrative Records	Known Best Practice	Operational Requirements	Legal requirements
Local area administrative records			
Timesheets	N/A	Retain for duration of current financial year	N/A
Leave/sickness	Statutory sick pay records not less than 3 years after the end of the financial year to which they relate	Retain copy for duration of current financial year. Forward original to HR	
Routine reports		Destroy 2 years	

FSA retention criteria for Administrative records			
Administrative Records	Known Best Practice	Operational Requirements	Legal requirements
Local area administrative records continued			
Minutes and agendas		Destroy 2 years	
Training		Details held on SAM database for duration of employment plus 6 years	
Disciplinary		Until discipline has expired, then papers passed to HR to retain in central record	
Local area administrative HoDs			
Budgets		Retain for duration of current financial year	
Training		Details held on SAM database for duration of employment plus 6 years	
Recruitment		Copy from HR held for duration of recruitment process then return to HR or destroy	
Disciplinary		Until discipline has expired, then papers passed to HR to retain in central record	
Routine reports monthly/quarterly		Destroy 2 years	
Team meetings		Destroy 2 years	
Bilaterals		Destroy 2 years	
Minutes and agendas		Destroy 2 years	
Emergency contacts		Continual update	
Letters and memos		Review/Destroy 1 years	
Sub contractors			
SC60 etc		6 years	6 years
Other income tax		6 years	6 years
National insurance	6 years	6 years	
Time sheets		Current plus 1 year	Current plus 1 year

FSA retention criteria for Administrative records			
<u>Administrative Records</u>	<u>Known Best Practice</u>	<u>Operational Requirements</u>	<u>Legal requirements</u>
Health and Safety			
Accident books		3 years from date of last entry	3 years from date of last entry
Control of substances hazardous to health		40 years from date of last incident	COSHH 40 years from date of last incident
Equipment inspection records		Varies according to equipment	Varies according to equipment
Risk assessments		3 years or until superseded	3 years or until superseded

Recommended Retention & Disposal practices

<u>National Archives Guidance on Retention and Disposal Schedules</u>			
<u>Type</u>	<u>Description</u>	<u>Disposal (maximum period)</u>	<u>Legislation that applies</u>
<u>Press & Public Relations Records</u>			
Dealing with the media and the public	Press Releases	7 years	
1			
2	Press Cuttings	1 month	
3	Operational notes(notices to press about forthcoming events or conferences)	3 months	
4	Press Conference reports/previews	3 years	
5	Press reports digests	7 years	
6	Correspondence with branches of the media	7 years	
7	Policy and administrative records	Second review (25 years)	
8	Handbooks and guides to media/public relations	Destroy when superseded	
9	Reports on media/public relations	7 years	
10	Image Library records	When no longer required	
11	Correspondence and papers	7 years	
12	Reports	7 years	
13	Visitor Books	3 years	
14	Calendars	3 years	
15	Brochures and Guides	3 years	

National Archives Guidance on Retention and Disposal Schedules		
Type	Description	Disposal (maximum period)
Contractual Records		
1	Policy on contracts, normally contained in a separate registered file series	First and Second Review
2	End user requirement	6 years
3	List of approved suppliers	An active document – updated regularly
4	Statements of Interest	1 year from date of last paper
5	Draft specification	Destroy when specification has been agreed
6	Agreed Specification	6 years from end of contract
7	Evaluation criteria	6 years from end of contract
8	Invitation to Tender	6 years from end of contract
9	Unsuccessful tender documents	1 year after date of last paper
10	Successful tender document	6 years from award of contract
11	Background information supplied by department	1 year after date of last paper
12	Interview panel – report and notes of proceedings	1 year from end of contract
13	Commissioning letter	1 year from end of contract
14	Signed contract	6 years from end of contract
		Limitation Act 1980 Unfair Contract terms Act 1977 Latent Damage Act 1986 Consumer Protection Act 1987 The retention scheduling for Building Records and Accounting Records is also relevant in the matter of the retention of Contractual Records

National Archives Guidance on Retention and Disposal Schedules		
Type	Description	Disposal (maximum period)
Contractual Records continued		
Contract operation and monitoring 15	Reports from contractors Schedules of works Bills of quantity (building contracts) Surveys an inspections	2 years from end of contract 2 years from end of contract 16 years
16		
17		
18	a) equipment and supplies b) buildings	a) 2 years from date of last paper b) Second Review
19	Records of complaints	6 years from end of contract
20	Disputes over payment	6 years from end of contract
21	Final accounts	6 years from end of contract
22	Minutes and papers of meetings	Second Review
Amendments to contracts		
23	Changes to requirements	6 years from end of contract
24	Forms of variation	6 years from end of contract
25	Extensions to contract	6 years from end of contract

National Archives Guidance on Retention and Disposal Schedules		
Type	Description	Legislation that applies
Health & Safety Records	<p>Only a small number of categories of records, including medical surveillance, accident and waste disposal records, have to be kept for a specified time. The most significant are listed below. In some cases, for example the Noise at Work Regulations 1989, assessment records should be kept until a further assessment of the hazard is made.</p>	<p>Health & Safety at work 1974, implementation of the requirements of the act are covered by these principal regulations: Safety Representatives and Safety Committees Regulations 1977 Electricity at Work Regulations 1989 Noise at Work Regulations 1989 Management of Health & Safety at Work Regulations 1992 Workplace (Health, Safety and Welfare) Regulations 1992 Health & Safety (Display Screen Equipment) Regulations 1992 Manual Handling Operations Regulations 1992 Provision and Use of Work Equipment Regulations 1992 Control of Substances Hazardous to Health Regulations 1994 (COSHH) Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR)</p> <p>The Social Security Act 1975 is also relevant to health and safety record keeping. Section 88(b) is the enabling provision under which relevant regulations are issued, such as the Social Security (Claims and Payments) Regulations 1979 and the Social Security (Industrial Injuries) (Prescribed Diseases) Regulations 1985. Other relevant legislation: Factories Act 1961 Employers' Liability (Compulsory Insurance) Act 1969 Fire Precautions Act 1971</p>
<p>Health & Safety records where there is a statutory requirement to keep records for a specified period</p>		

National Archives Guidance on Retention and Disposal Schedules		
Type	Description	Legislation that applies
Health & Safety Records		Control of Substances Hazardous to Health Regulations 1997
List of employees exposed to group 3 and 4 biological agents (see the Regulations)	10 years after last exposure	Reg 7 (10) – special provision relating to biological agents
Where exposure may lead to a disease many years later	40 years after last exposure	Schedule 9 – special provision relating to biological agents
Examination and testing of control equipment and repairs carried out as a result	5 years	Reg 9 – maintenance, examination and test of control measures
Exposure to hazardous substance at the workplace: a) general exposure b) personal exposure of identifiable employee	5 years 40 years	Reg 10 – monitoring exposure at the workplace
Health surveillance, including medical reports	40 years from date of last entry	Reg 11 – health surveillance of employees who are, or are liable to be, exposed to a substance hazardous to health
General Register Form F31, recording details relating to the factory, such as name and address of occupier, nature of work, fire certificate, etc	2 years from date of last entry	Factories Act General Register Order 1973
Reportable injuries, diseases and dangerous occurrences	3 years	Reporting of Injuries, Diseases and Dangerous Occurrences Regulations

				1995 (RIDDOR)
National Archives Guidance on Retention and Disposal Schedules				
Type	Description	Disposal (maximum period)	Legislation that applies	
Health & Safety Records continued				
Accident book (form B1 510)		3 years from date of last entry	Social Security (Claims and Payments) Regulations 1979	
a) health records		50 years from date of last entry	The Ionising Radiations Regulations 1985	
b) examination of respiratory protective equipment		2 years		
Radiation passbook		5 years after finish of use	The Ionising Radiations (Outside Workers) Regulations 1993 Control of Lead at Work Regulations 1980	
Maintenance of control measures		5 years from date at which last entry was made	Reg 8 (4) – maintenance, examination and test of control measures	
Air monitoring		5 years	Reg 9 (5) – monitoring exposure	
Medical Surveillance		40 years from date at which entry was made	Reg 10 (3) – health surveillance of employees exposed, or liable to be exposed, to lead	
Health surveillance (including medical reports)		40 years after last record	Control of Asbestos at Work Regulations 1987	
a) health surveillance		40 years from date of last entry	Work in Compressed Air Regulations 1996	
b) exposure		40 years from date of last entry	Special Waste Regulations 1996	
Consignment note		3 years	Environment Protection (Duty of Care) Regulations 1991	
Consignment (controlled waste)		2 years		

A large, light green, stylized number '9' is positioned on the right side of the page, extending from the top to the bottom. The number is composed of thick, rounded strokes and is set against a white background.

The Financial Services Authority
25 The North Colonnade Canary Wharf London E14 5HS
Telephone: +44 (0)20 7066 1000 Fax: +44 (0)20 7066 1099
Website: <http://www.fsa.gov.uk>

Registered as a Limited Company in England and Wales No. 1920623. Registered Office as above.