



RECORDS MANAGEMENT MANUAL

Supporting the Agency's Information Management Needs

Produced by Records Management
Version 4.0/ June 2007

Table of Contents

INTRODUCTION TO INFORMATION MANAGEMENT.....	3
THE STANDARD FOR RECORDS MANAGEMENT FOR THE TREASURY SOLICITOR'S DEPARTMENT.....	6
PRODUCING DOCUMENTS AND DECIDING WHAT TO DO WITH NEW INFORMATION.....	11
REGISTERED FILES - INTRODUCTION.....	12
REGISTERED FILES - HOW TO OPEN.....	14
REGISTERED FILES - HOW TO USE.....	17
REGISTERED FILES - HOW TO CLOSE.....	20
FILE RETENTION AND DISPOSAL POLICIES AND PROCEDURES.....	23
FILES ON LOAN FROM THE FILE STORE.....	25
ELECTRONIC RECORDS, E-MAILS AND ELECTRONIC.....	26
FAX MESSAGES.....	26
PERSONAL AND TEAM REFERENCE MATERIAL.....	29
STORAGE OF PAPER RECORDS AND OPERATING THE CLEAR DESK POLICY	30
MANAGING INFORMATION PUBLISHED THROUGH OUR FREEDOM OF INFORMATION PUBLICATION SCHEME.....	33
REQUESTS FOR ACCESS TO INFORMATION.....	37
RECORDS MANAGEMENT PROCEDURES FOR THE PRIVATE OFFICE.....	39
THE MANAGEMENT OF PUBLIC INQUIRY RECORDS AND OTHER TEMPORARY BODIES.....	43
Appendices.....	47
<i>Appendix 1</i> - Deciding what to do with new information - flow chart.....	47
<i>Appendix 2</i> - Request to open a new file.....	48
<i>Appendix 3</i> - Standard prefixes in use in the Agency.....	50
<i>Appendix 4</i> - File index form.....	52
<i>Appendix 5</i> - Record of Disbursement (Finance Certification).....	53
<i>Appendix 6.1</i> - Retention schedules for Advisory, Bona Vacantia and DOCS.....	54
<i>Appendix 6.2</i> - Retention schedules for Litigation, COCAD & ECCG.....	58
<i>Appendix 7</i> - File Closure Checklist Label.....	66
<i>Appendix 8</i> - Form for the front of bundle of papers that do not fit into a file jacket (in case files).....	67
<i>Appendix 9</i> - Guidance Notes on using the Current File Store and Forms to be used.....	68
<i>Appendix 10</i> - The Agency's Code of Practice for Data Protection.....	71
<i>Appendix 11</i> - Retention Policy for Private Office records.....	78

INTRODUCTION TO INFORMATION MANAGEMENT

Purpose: *To introduce the Agency's Information Management Standard and the supporting series of desk-notes. It puts information management in context with the surrounding legislative framework and the business of the Agency, and explains how you will benefit from meeting the standard.*

- 1 The Agency's Information Management Standard is set out in a series of desk-notes. The desk-notes each cover a specific aspect and include tips to help you meet the Standard. Collectively the desk notes are the department's records management policy.

For COCAD, European and DOCS Divisions, please also refer to the [eRIK User Guide](#). This sets out the rules and procedures for using TSol's Electronic Records Management System (EDRMS), which is named eRIK (Electronic Records and Information Knowledge).

- 2 The key is for the right information to be where it is needed, when it is needed. Meeting the Standard and using the systems provided to the full will give you more time to do your job, because you will spend less time looking for information. You will spend less time addressing issues that have already been addressed. The time you spend managing information, will always save you time in the long run.
- 3 **Meeting the Standard is not optional.** It applies to all parts of the business performed by the Agency, and all staff, wherever they are based. It applies to all recorded information, no matter what format it is in.
- 4 Specific aims of the information management standard are to ensure that all the Agency's records are managed in accordance with the requirements of:
 - The Public Records Acts 1958 and 1967
 - The Data Protection Act 1998
 - The Freedom of Information Act 2000
 - The Environmental Information Regulations
 - information providing evidence of the Agency's functions, policies, procedures, decisions, actions and other key activities are recorded
 - the Agency knows what records exist
 - records can be retrieved promptly to aid decision making
 - records created for the Agency's purposes are adequate, relevant and not excessive
 - records created or received by the Agency are retained for the minimum period of time consistent with its value as a record of its policies and activities for accountability purposes
 - those records worth preserving permanently, because of their administrative, research or historical value, are identified, safeguarded and ultimately transferred to the National Archives
 - that records retained under the Agency's control are stored and managed economically and in such a way that they can be retrieved readily, reviewed, regularly and disposed of promptly

- 5 The Standard reflects the fundamental importance of the Agency's need for reliable, complete and retrievable records through efficient and effective records management, to enable it to achieve its aim to provide its services efficiently and economically, and to draw on past experience.
- 6 The legislative framework surrounding information is increasing in complexity and scope. The standard, and supporting guidance is based on these authorities and reflects what is widely considered as best practice.
- 7 Let's be clear about what a record is. A record is evidence of TSol activity or a TSol transaction, which is used to support a TSol activity, decision or transaction. It can be helped in any format, including electronically, or on paper, audio or videotape, microform, film or another media. The terms 'record' and 'information' are used interchangeably throughout the desk-notes to describe recorded information.
- 8 Records Management is about managing information from the moment it is received or created, until it is destroyed or transferred to another organisation, as evidence of action so that its existence is recorded, it can be found quickly when needed and it is stored and managed economically. It is **not about 'dead'** records. Nor is it just about archives or dormant records. It is very much about live, essential records. Records Management is something that all of us do all the time at work and at home. Provided we think about what we are doing, and follow good practice, our records will support us.
- 9 A word of warning. If you manage records badly you will affect the performance of the Agency, your colleagues and yourself. Bad records management may lead to:
 - poor or inconsistent decisions being made
 - duplicated effort - re-inventing the wheel
 - poor working environment
 - time wasted searching for information
 - losing a legal case
 - wasted office space
 - inability to recover from a disaster, such as a fire or flood

Roles and responsibilities

- 10 All of us in the Agency are responsible for records management. It is not the responsibility of one person, or a particular group of people.
- 11 **All staff** are responsible for meeting the Standard for the records they receive and create, and for which they are accountable.
- 12 **The Division or team** with responsibility for a case or policy has responsibility for maintaining the official record documenting that function. They must have procedures in place to ensure that they are able to identify, trace and control all documents and other information relating to that matter, and that these are properly stored.

- 13 **Managers** are responsible for seeking the advice of the Head of Records Management whenever:
- changes to the format of records are planned
(e.g. electronic records management or document imaging projects)
 - significant new collections of records are created
- 14 Managers are responsible for ensuring that their staffs are given sufficient training in records management to enable them to do their jobs well.
- 15 **The Head of Records Management**, referred to in the Public Records Act as the Departmental Record Officer, is responsible for supporting the efficiency and quality of Agency's business and ensuring compliance with legislation and guidelines surrounding information. He will do this by formulating and advising on Departmental standards for the effective management of information.
- 16 The Head of Records Management has the right to examine any record to determine whether it is being managed in accordance with the Standard and whether it should be preserved as a Public Record.
- 17 Other members of the Records Management team are responsible for registration of new files; review, disposal and transfer of records to the National Archives; providing a file storage and retrieval service. Together with the Head of Records Management the team provides a consultancy service for all aspects of information management.

THE STANDARD FOR RECORDS MANAGEMENT FOR THE TREASURY SOLICITOR'S DEPARTMENT

Purpose: *The Agency's Standard for Records Management. It consists of broad policy statements, which are expanded in the supporting desk-notes.*

Overall Policy Statement

The Agency will manage information it creates or receives in accordance with the requirements of the Public Records Act 1958 and 1967, Data Protection Act 1998, Freedom of Information Act 2000 and the Environmental Information Regulations at all times, and will keep well ordered records of it's actions in a corporate filing system.

The Standard for Records Management

All staff in the Agency must follow this standard, whether they are based at One Kemble Street or assigned to other Government departments. It will be monitored through audits and inspections.

Corporate filing system

- 1 The Agency will operate a structured corporate filing system, with Registered Files being distinctly separate from reference material.

Registered Files (for non eRIK Users)

- 2 The division, team or officer with responsibility for a case, policy or administrative area will maintain the official record documenting that function on a Registered File as a full record of events in a logical order.
- 3 Documents created or received electronically will be printed to paper if they have value and record a decision or action, or provide background information to a decision or action.
- 4 Standard file jackets only will be used for Registered Files.
- 5 A separate file will be opened for each case or topic, and annual files will be opened for those topics, which could potentially continue indefinitely.
- 6 Information recorded on the front of the file will always consist of at least the minimum standard of: file reference, title, case holder, date opened, date closed, disposal directions and chargeable client.
- 7 All documents on a subject, or topic, will be grouped together on a file on that topic.
- 8 Each file will be given a clear and descriptive title that reflects the subject of the contents.

- 9 Each file will be given a unique reference, including a prefix identifying the work area, in a format agreed with the Head of Records Management.
- 10 Only prefixes agreed with the Head of Records Management will be used.
- 11 A tracking system will be operated to ensure that the current location of every Registered File is recorded, and that the file can be located quickly.
- 12 A computer index will be maintained, recording the existence of every Registered File, to include:
 - file reference
 - series
 - file title
 - date of opening
 - date of closure
 - retention or disposal directions.

Contents of Registered Files

- 13 The contents of any one team's Registered Files will be organised by all members of the team in a common order agreed and accepted by them all, e.g. chronological order.
- 14 Where appropriate loose documents should be secured with a treasury tag.
- 15 Items that cannot be secured with a treasury tag, such as audio and videotapes, will be held inside envelopes, with the file reference and description of the contents on the outside, which will be secured with a treasury tag.
- 16 File contents will be indexed, where appropriate, particularly in large cases or matters.
- 17 All teams will set and manage targets for placing material created or received on the file to which it relates. A target of within three days of creation or receipt is suggested.

Electronic Records (for eRIK users)

- 18 Electronically produced documents, e-mails and faxes that record a decision or action, or add value to a decision or action, that have been produced using eRIK should be placed on the electronic file to which they relate, by the person with responsibility for maintaining the file.
- 19 Paper components to electronic files will need to be created to contain any paper documents. The paper component of the file must be cross-referenced with the electronic file (see eRIK User Guide –Chapter 5 Managing Physical folders and Physical Items)

Dormant files

- 20 Files will be closed when all foreseeable action on them has been completed, and all outstanding monies settled.
- 21 Paper files relating to Agency policy and administrative matters will be closed, at the latest, five years after they were registered.
- 22 Files and all accompanying papers will be prepared for storage in a standard departmental format. This applies particularly to papers that do not fit the jacket of the paper file component.
- 23 Paper files, or file components, will be stored in the File Store when they have been closed, and are not needed regularly (e.g. weekly) for reference.
- 24 The files will be organised so that every one can be retrieved quickly, and those ready for review or destruction are easily identified.
- 25 Closed files on loan from the File Store should be returned once they are no longer needed regularly for reference.

Retention and disposal of Registered Files

- 26 Standard departmental retention schedules will be in place for all records and will be followed.
- 27 The periods shown on the retention schedules will be taken to run from the date that the file was first closed, and destruction or review will take place once that period has passed.

Protocols for creating documents

- 28 Version control of documents will be managed in the following way:
Documents produced in draft will be clearly marked as 'draft', followed by 'version' and the version number (starting with 1 for the first), and ending with the date, for example 'Draft Version 1-2/3/00' for the first version of a draft document produced on 2 March 2000. The final version will be marked with 'version', followed by the version number and the date. These should appear in the top right-hand corner of every page as a header.
- 29 Every document produced by the Agency whether for internal or external readership, will include the reference of the file to which it relates.
- 30 Every document or e-mail produced in the Agency will include a heading describing the broader and narrower subject of their content.

Reference material

- 31 A separate system will be operated for personal reference material and team reference material, which will be distinctly different to that for registered files. This will be used to hold information sent for reference, or produced by the user in a matter in which they do not have the lead, and therefore do not have the Registered File.
- 32 Reference material will be shared as much as possible, and will be organised in such a way that retrieval of information on a topic is quick and easy.
- 33 Material retained for reference, but not as an official record may be held electronically on a shared drive, provided all potential users have ready access.
- 34 Reference material will be reviewed every six months, and destroyed when it is out of date.

Security

- 35 A clear desk and clear screen policy will be operated. The clear desk and clear screen policy means that all sensitive **papers** are locked away, and access to computers and floppy disks controlled when the office is unoccupied. Sensitive papers are those **containing any information at all relating to the Agency's work.**
- 36 The cover of a registered paper file will indicate the highest protective marking of any document held on it (see the staff handbook for guidance on the use of protective markings). Any document containing information that is marked above "Restricted" must not be held electronically and should be held in paper format within a paper file jacket.
- 37 Protective markings assigned to a file will be reviewed regularly (every six months is suggested), and always before the file is closed, and will be downgraded or removed when appropriate.

Storage

- 38 Cupboards, preferably with roller shutter doors, should be purchased in preference to filing cabinets, because such a cupboard will provide almost twice as much storage space occupying the same amount of floor area.
- 39 Cupboards should be fitted with the maximum number of shelves allowing for files to be stored on their spines.
- 40 Storage space will be used efficiently, with team-based filing where appropriate. E.g. Files should be stored on their spines, rather than flat.
- 41 Files will be stored in a standard order by all members of any one team, such as reference order.

Monitoring

42 The Head of Records Management will be informed of:

- all information systems, manual or computerised, their purpose and the types of records held, so that decisions can be made about appraisal of such records under the requirements of the Public Records Acts
- all new IT applications, their purpose and the types of records held
- all new collections of paper files, for a purpose not previously held by a particular team

PRODUCING DOCUMENTS AND DECIDING WHAT TO DO WITH NEW INFORMATION

Purpose: *To help you make the management and use of records easier for yourself and your colleagues, and help you to decide what to do with new information you create or receive.*

Producing documents

- 1 It is important to bear in mind that information we record in the course of doing our jobs might be seen by people outside of the Agency. The Freedom of Information Act, Environmental Information Regulations and Data Protection Acts give the public the right of access to information we hold, subject to certain limited exemptions. Care should be taken to ensure that information recorded is accurate, is not offensive and could not be misunderstood.
- 2 Documents produced in draft will be clearly marked as 'draft', followed by 'version' and the version number (starting with 1 for the first), and ending with the date, for example 'Draft Version 1 -2/3/00' for the first version of a draft document produced on 2 March 2000. The final version will be marked with 'version', followed by the version number and the date. These should appear in the top right-hand corner of every page as a header.
- 3 Every document produced, including e-mails, should have a clear broader and narrower description of the subject before the message. This will tell the reader at a glance what it is about.
- 4 Every document produced by the Agency, whether for internal or external readership, should include the reference of the Registered File to which it relates. This should encourage the recipient to use it in any subsequent correspondence, and will make it easier for users to find the file.

Deciding what to do with new documents

- 5 When a new document is created or received you must decide whether it needs to be placed on a registered file. The flow chart at [appendix 1](#) should help you to make this decision.
- 6 If the document is either ephemeral (of short-term value, e.g.; advertising literature, printed material etc); or not the functional responsibility of you or your team it should not be placed on a Registered paper file component.
- 7 If the information relates to your function and is not ephemeral you must decide whether an appropriate Registered File already exists. If no appropriate file exists, it will be necessary to create one with a reference and a title.

REGISTERED FILES - INTRODUCTION

Purpose: *To explain when Registered Files should be used. This applies to all parts of the Agency.*

- 1 Registered Files are used to hold the Agency's official and primary record on any subject and are its primary information resource. In effect they are used to provide evidence of the Agency's business transactions.
- 2 The Division, team or person with responsibility for a case, policy or administrative area has responsibility for maintaining the official record of it on a Registered File. For example, Facilities Management will hold records relating to the maintenance of the accommodation on a registered file, since that team is responsible for that work.
- 3 Registered files will be used to record every area of the Agency's work. This will consist of:
 - The formulation or modification of the Agency's policies or practice, which will be applied to individual cases or instances
 - The application of the Agency's policies or statute to individual cases or instances
 - Administration of the Agency, such as budgetary and matters relating to the management of the Agency.
- 4 The aim is that all information relating to a topic, or matter will be held together within one Registered File, or group of related files, so that the full story can be seen by the reader, without them having to hunt for information from a number of sources. It should be clear how the matter has evolved, and what action is still outstanding.
- 5 The following information should be held on Registered Files by the Division or team **with responsibility for the function:**
 - incoming correspondence
 - a copy of outgoing correspondence
 - decisions made by staff in the Agency, and action taken in relation to those decisions
 - a full set of papers relating to the correspondence or decision, which will give the background and reasoning behind it, and provide supporting information (this could include notes or minutes of meetings)
 - papers and minutes of any departmental, or inter-departmental working group or committee
 - internal policy or administrative guidance
 - the Agency's manuals, directories and publicity material
 - financial management and budgetary information
- 6 This arrangement is a requirement of the Public Records Act 1958 and reflects the accountability of:
 - individuals (as civil servants)
 - the Agency (as a government Department) for its actions.

Staff assigned to other Government Departments

- 7 Staff who have been assigned to other Government Departments must meet the Agency's standard for Records Management, even if the host department's files are used. The files can be registered by the client department.
- 8 The reason for this requirement is that the Agency is responsible for ensuring that the decisions made by all of its staff are recorded on official files. Those files belong to the Agency and not to the host departments. This applies even when the host department carries out file registration for the Agency.
- 9 Files registered by the client department on behalf of the Agency's staff should be sent to the Agency when they are no longer needed for reference.

Time recording and direct billing

- 10 File registration is an integral part of the Agency's time recording and billing system, which produces our invoices for client departments. Until a case is registered, and a chargeable client identified, no work can be charged against it.

REGISTERED FILES - HOW TO OPEN

Purpose: *To explain the procedure for arranging for a Registered File to be opened by the Records Management Team. The procedures described do not apply to those divisions that register their own files, but the principles are relevant to all parts of the Agency.*

Creation of paper files

- 1 Some registered paper files for the Agency are opened by Records Management, others are opened by teams within Divisions. In addition some Advisory Divisions have made arrangements for their host departments to open files for them.
- 2 At [appendix 2](#) is a copy of the form that should be used to request a new file from Records Management. It is essential that all details given are complete and accurate to aid retrieval of the record, and to avoid incorrect billing. If a continuation file is being requested, details of the part number needed should be entered.
- 3 Completed forms should be sent to RM Registry (Zone 5.10) either by post or email to registry@tsol.gsi.gov.uk.

Creation of electronic files (for eRIK users)

- 5 Electronic Files will be created by Divisional teams and not by Records Management.

Turn-around times

- 6 Records Management will aim to produce file jackets within one working day of receipt of the request but if a new file is needed urgently it can be requested by telephone to Registry.

File Front Sheets

- 7 Only file front sheets approved by Records Management may be used in the Agency.
- 8 Information recorded on the front of the file should always follow the standard format, to include as a minimum: file reference, title, case holder, date opened, date closed and disposal directions and chargeable client.

File reference

- 9 Each registered file is given a unique reference. Those opened on Datix will consist of:

- a prefix to reflect the broad work area that the file supports
- the last two digits (for pre-2000) or last digit (for post-2000) of the year of registration
- a sequential number to reflect the files position in the system
- a check digit at the end

File Prefixes

- 10 Other registered files opened in the agency will use prefixes shown at [appendix 3](#). These are controlled by the Head of Records Management. No new series may be used by staff employed by the Agency, whether at OKS or assigned to other Government Departments, without the approval of Records Management, even when the files are registered for Agency staff by the host department. This is to ensure adequate file management and to prevent duplication of file prefixes.

Subject based files

- 11 Each file should deal with a single subject. There should, usually, be only one file on a specific topic, or aspect of it within the Agency. Too many small files on a subject make it difficult to see what is going on. Equally if a file covers too many issues it is difficult to follow the story. eRIK provides users with the opportunity to share access to files across the Agency thereby facilitating a reduction in the creation of several similar case files.
- 12 Where appropriate a file may cover more than one matter, such as one of advice to a particular government department when it would be impractical to open a separate file for each advice matter. In such instances a new file should be opened every year, and previous files closed. This will meet the requirement of the Public Records Act that **no files are open for more than five years**, and ensures that the mechanisms for review and transfer to the National Archives are not frustrated.
- 13 If a file grows too quickly it might be an indication that there is a need to break the file down into a number of more specifically titled files, or that the contents of the file now go beyond the scope of the original title.
14. For those subjects that are ongoing over many years, and which it would be impractical to break down into separate files by case or action, annual files should be used. This will limit the growth of a file, and will allow for earlier documents to be destroyed in line with departmental retention policies. It will also make it easier for users to find specific information on the file.

File titles

- 15 The purpose of a file title is to describe the subject of the contents of the file, and to limit the scope of the material placed on it. It should be as concise as possible, whilst providing accurate information about the actual and likely contents of the file. At the same time it ought to be sufficiently restrictive to discourage users from using the file to cover different developments of the original subject, which really ought to be the subjects of several files.

- 16 The title must contain key words relating to the subject of the papers contained within the file. Keywords should be chosen and structured in such a way as to make searching and retrieval easy and straightforward.
- 17 The use of non-specific or generic terms, such as 'general correspondence' and 'miscellaneous' must not be used. Files with such titles will inevitably become dustbins, with no real use to any user when they are looking to retrieve information. Electronic file retrieval would become problematic if such terms were used.
- 18 Acronyms and abbreviations used in the title must be those in common use within the whole of the Agency, otherwise the words should be written in full.

Protectively marked files

- 19 Where a file warrants a Protective Marking above Restricted, i.e. Confidential, Secret or Top Secret (as defined in the Staff Handbook), it should not be recorded on a database or any other list to which others not aware of the case or matter would have access. For example, DATIX should not include details of the title that would give away Protectively Marked or sensitive information. Instead the database or file list (e.g. DATIX) should be given the general title 'TITLE WITHHELD', and the file will be recorded on a separate secure database held by Records Management, to which only Records Management will have access.
- 20 Electronic files (eRIK). Documents above the Restricted marking should not be stored within eRIK but should be printed to paper and held within a paper file jacket.
- 21 The file title will be recorded on the front of the file jacket in the usual way, but will be sent under cover, as appropriate for the level of protection required for the marking.
- 22 The 'holder' of the file is responsible for storing it in appropriately secure conditions, again as defined in the Staff Handbook.
- 23 Where the parent file has been created electronically, papers marked Confidential, Secret; Top Secret must be held within a paper file jacket marked with the appropriate security marking. The electronic database should not record the fact that material above "Restricted" is within the paper component.

REGISTERED FILES - HOW TO USE

Purpose: *To explain how Registered Files should be used to meet the legislative requirements and work for you. It includes filing protocols, and applies to all parts of the Agency, whether or not the files are registered by Records Management.*

Filing documents on registered files

- 1 Incoming letters, copies of outgoing letters, minutes, reports etc should be placed on the paper file. They should be secured with a treasury tag in an order that has been agreed at team level, and has been agreed by all members. Chronological order may be appropriate.
- 2 Those documents that should not be hole-punched, and items that cannot be secured with a treasury tag, such as audio and videotapes, should be placed in an envelope, with the file reference written onto it (in case it becomes detached from the file). The envelope should then be tagged in the file. This will reduce the risk of papers becoming lost.
- 3 For eRIK users, outgoing letters, emails etc, should be held on the electronic parent file. Incoming letters and other paper documents should be held within a paper file jacket.
- 4 Originals of documents that have been scanned must be retained within a paper file jacket.
- 5 Documents should be added to the file to which they relate as soon as possible after they are created or received. Teams should set and manage targets for this. A target of within three days of creation or receipt is suggested. This will mean that whoever picks up the file can see the latest position quickly.
- 6 Files, rather than individual documents, should be sent between members of the same team. This will ensure that the contents are kept together, and readers can see the full picture. The risk of individual documents becoming lost would be reduced.

Index to contents of paper file

- 7 The contents of the file should be indexed (a form is copied at [appendix 4](#). The index should include:
 - a sequential number to each document (identifying it's place in the file)
 - the date of the document
 - the name of the sender/recipient
 - a brief description of the narrow subject matter of the document.
- 8 The enclosure number should be written in the top right hand corner of the document and the number circled. An index form will be included in every file supplied by the Records Management.

- 9 The index will make it much easier to find individual documents on a file, and so gives a potted history of the work done so far. After all it can be very irritating to pick up a file containing masses of paper, and having to wade through it to find the document you need. It is far easier to look at the index. Time spent on indexing is more than balanced against the time that will be saved looking for documents.

Adding new papers to a file/changing the title

- 10 Care must be taken to ensure that the file title continues to reflect the contents accurately. It is better to create a new file for new papers when they take the subject beyond that described in the title. The files can be cross-referenced if necessary. It is unwise to change the title of an existing file unless absolutely necessary, because users become familiar with them and changing them is almost bound to lead to confusion.

Recording developments

- 11 Every file needs to show the full picture of the matter they record, and provide a full record of the events and actions. Decisions, events and conversations (including those over the telephone), which have a bearing on the case or topic should be recorded and placed on the file when they are not recorded elsewhere. The record should be made on a relevant document or separately if it does not relate to an existing document. For case files the record should be made on attendance notes together with units of time worked. It should be indexed as any other document. Post-it notes should not be used, because they can become detached, and which could lead to important information being lost.

Continuation or Part File - if a paper file becomes full (this does not apply to electronic eRIK files)

- 12 If it is necessary to add new papers to a file that has become full a new 'part' file should be opened. This would be given the same reference as the first file, but with the 'part' number written onto it. These should be requested in the same way as any new file, and is described in Records Management Desk-note Number 5. Continuation/part files should always be produced by Registry. You should not make your own. You should tell Registry the number of the next part file you need.
- 13 When a case or matter is going to generate a lot of paper, it is not necessary to open a file for all papers. However, separate bundles should have an indicator to the reference and title of the file to which they relate on the top of them.
- 14 Continuation/part paper files should only be opened if there are too many papers to fit on the original file. If it is evident that a new aspect of the case has come about, a new case file with a new file reference must be created. Even if elements of a case are common to one which already exists, for example, the same parties but a different case, a new file must be opened.

Re-allocating cases

- 15 Team Leaders are responsible for re-allocating cases promptly when a member of their team leaves their team. (See instructions below about making sure that DATIX is updated to reflect changes in file details.)
- 16 The team member with responsibility for the file must pass it over to the new team member in a well-organised condition and with all records on it.

File tracking

- 17 Accurate recording of all paper file movements is essential if information is to be located quickly. One of the primary reasons for files being lost is because movements have not been recorded. The success of the tracking systems depends upon the people using it.
- 18 Tracking of records is required to:
 - enable the quick retrieval of the record
 - monitor use for the maintenance of systems and security
 - maintain an audit trail of records transactions, such as registration, classification, access and disposal.
- 19 The tracking system should show the current location of every paper file.
- 20 The team secretary, or Records Management for COCAD & European teams, must be told when responsibility has passed from one case holder to another, so that DATIX can be updated.

REGISTERED FILES - HOW TO CLOSE

Purpose: *To explain the procedure for closing Registered Files. It includes tips for reducing work in the future. The procedures described do not directly apply to those divisions that register their own files, but the principles of closing files apply to all parts of the Agency.*

When to close a file

- 1 A file should be closed when all foreseeable action has been completed, outstanding monies have been settled and no further correspondence is expected. (Once closed the paper file can be returned to the user, if they require access to it frequently. The electronic eRIK file will remain on the system until it is destroyed).
- 2 Files recording the Agency's policies and their development or the administration of the Agency should be closed at the latest five years after they are registered (opened). This prevents papers being added to the file indefinitely, and prevents the timing of review and transfer to the National Archives being frustrated. The same principle applies to the closure of electronic files.

How to close a file

- 3 The Record of Disbursement (finance certification) inside the front of the file cover must be completed for all case files. See [Appendix 5](#) for a copy. This is a National Audit Office requirement. It ensures that no finance, costs and disbursements are overlooked. Before signing and dating it case holders are responsible for checking the papers to establish that, for example, receipts for compensation payments are on file, or that counsel's or agents fees have been paid and acknowledged and all relevant debt monies have been recovered and passed to clients. Case holders are not expected to check that the client has paid the bill issued by business support.
- 4 It may be appropriate in some cases to consider obtaining authority for costs to be written off, in accordance with Divisional procedure. Where costs have been awarded against our client, but no bill of costs has been rendered, it may seem that no certification can be given. However, under the Rules of the Supreme Court, a bill of costs must be lodged within three months of the order, or the receiving party is at risk of having the costs disallowed in total or in part. Below is the text of a note, which may be copied, completed and placed on the correspondence file to enable the case to be archived. The costs certification on the front of the file should be marked 'see inside' to draw attention to the note.

NOTE FOR THE FILE

'By an order dated.....the Secretary of State was ordered to pay costs in this case.

By virtue of Order 62 Rule 29(1) RSC', a party entitled to costs has three months from the date of the order to lodge his bill of costs. If he fails to do so, all or parts of his costs may be disallowed on taxation.

At the date of archiving of this file, no bill of costs has been received. The file is therefore marked for destruction ten years after the date of the order.

*In the unlikely event of the Bill of Costs being lodged after the file has **been** destroyed the agency will be justified in applying to have it disallowed in its entirety on the basis that the other side 's inordinate delay has irretrievably prejudiced the Secretary of State.'*

Duplicates and drafts

- 5 Duplicate documents should be destroyed before the file is closed, be they paper or electronic. As too should any draft documents that do not illustrate key developments in the matter, or important views on the content, once the final version has been produced.

Disposal Directions

- 6 Before sending a paper file for closure the disposal directions box on the front must be completed. The departmental retention schedule is copied at [Appendix 6.1](#) and [6.2](#) and contains guidance on appropriate retention periods agreed within the Agency for files handled by Litigation, Advisory and Bona Vacantia Divisions. Please see Records Management Desk-note number 8 for advice on selecting the most appropriate disposal directions, and for a fuller description of the procedures for review and disposal of files.

The File Closure Checklist label, attached to the back of the file must also be completed before a file is sent to the File Store- See [appendix 7](#)

- 7 Make sure the file is complete, and all related papers (including correspondence) are sent to the File Store with it. This excludes additional 'part' files, which may be kept open when earlier parts have been closed and sent to the File Store
- 8 Once the disposal directions have been written onto the paper file, and all other action described above has been completed the file should be sent to the File Store (Paper Room), where it will be recorded as closed on DATIX, and put into storage.

Over-size paper files

- 9 Where papers do not fit into the file jacket a standard form ([appendix 8](#)) must be completed and attached to the front of the bundle. The bundle, which for health and safety reasons should not be more than 5 inches (12cm) deep, must be secured by cotton tape across the shorter and longer dimensions and tied with a bow at the front. This will reduce the risk of papers being misplaced in the File Store. It will also mean that individual documents can be more easily retrieved by future users, and will make it easier for users to handle the papers.
- 10 For policy and administrative matters part paper files should be used for all additional papers, instead of loose bundles of papers.
- 11 The File Store will reject any bundles that have not been prepared to this standard.

Continuation/Part Files

- 12 Only the final continuation part paper file should be signed-off, because all files bearing the same reference should effectively be treated as one, and if any are still being worked on none should be signed off.

Adding correspondence to a closed file

- 13 When unexpected correspondence is received and needs to be added to the file it can be sent to the File Store. It should be marked 'for filing'. The Agency's reference should be written clearly in the top right hand corner on the front page, if it has not already been typed on the document. The File Store will aim to link such correspondence to the file within two working days of receipt.

FILE RETENTION AND DISPOSAL POLICIES AND PROCEDURES

Purpose: To set out the Agency's file retention and disposal policies, and explain how these are operated to help you prompt the most appropriate disposal action.

- 1 The Agency's standard file retention periods are set out in the schedule at *Appendix 6*. The schedule will be enlarged over time to include all work areas. The retention schedule is based on the Agency's likely need in respect of the various categories of files it opens.
- 2 When a file is closed the Case holder should consider it against the retention schedule, and decide if the period set out in it is appropriate. If it is they should write it onto the file.
- 3 **The retention periods shown on the schedule run from the date of the most recent paper on the file when it was closed.** Files will be destroyed without review unless one of the preservation or review options are chosen by the Case holder marking the disposal directions on the file. When a file has been retrieved from the File Store and then returned to storage the disposal directions will not be changed unless a note is written next to the existing disposal directions on the front of the file.
- 4 Exceptionally, it may be necessary to assign a longer retention period than that set out in the retention schedule. If a longer retention period is required a brief note setting out the reasons should be attached to the front of the file.
- 5 Shorter periods should not be used without the approval of the Head of Records Management.
- 6 The options available on the front of the paper file are:
 - **Destroy after X** years - This option should be selected if it is clear that the file could safely be destroyed, **without review**, after the period set out in the retention schedule (or a longer period if appropriate) The appropriate period should be written into the space provided, and shown as X above.
 - **Preserve** - This option should be selected if the file contains information that is so valuable that it will be required for reference beyond second review (which takes place twenty five years after the file was registered).
 - **Consider at First or Second Review** - this option should be chosen if the file should not be destroyed without review. Second Review should be selected if it is apparent that the file will be required beyond the next five years. First Review takes place at the end of the standard period shown on the retention schedule.

7 The following types files should be marked for first review

- Precedents
- Unusual cases or matters
- Matters which have been referred to the House of Lords
- Cases involving famous or notorious people, or notable events
- Cases which attract significant coverage in the national media
- Matters which are likely to have reference value beyond the period set out in the retention schedule
- Matters relating to a major policy area of the Agency, or advice by the Agency on a major policy area or legislation to another government department.

Precedents

8 If a case is a precedent it must be clearly marked on the front of the file, and it should be marked for first review.

Review and disposal

9 Records Management will carry out first and second reviews on those records marked for review, in line with the acquisition policies of the National Archives. When deciding whether to keep a file for longer or to destroy it we will ask ourselves:

- does the record have any historical or research value (e.g. is it an important case or does it involve an important person or event, or a development in the work or structure of the Agency)
- does the record have continuing administrative value (in which case it is likely that it will be required for reference)

10 Files retained at second review will either be transferred to the National Archives or will be retained in the department for a definite period because they have continuing administrative value (for this we would need the approval of the Lord Chancellor).

11 Records Management will keep a record of all files destroyed.

FILES ON LOAN FROM THE FILE STORE

Purpose: *To set out the procedure for retrieving a closed file from the File Store*

- 1 When you require a file to be retrieved from the File Store you should send your request via e-mail to 'Paper room', or in writing via the messenger service. Requests sent via the messenger service will be slower than requests sent via e-mail. Your request should include the following information to enable the File Store to retrieve the correct file:
 - the file reference number
 - the case name, or file title
 - the name of the person in the Agency to whom the file should be sent
 - their room number.
- 2 There are two deliveries a day by the File Store to the messengers' room at 10.30am and 14.30pm. E-mail messages will be checked four times a day for delivery on the next round.
- 3 Any exceptional requests which require greater urgency than the time set out above allow should be made on the telephone to the File Store.
- 4 Files should be returned to the File Store once they are no longer required for reference, and they should be kept in their original, or better order.
- 5 If you transfer the file to someone else you should inform the File Store by completing the tear off-slip at the bottom of the standard minute that they attach to the file. This will enable them to update the tracking system, so that you and your colleagues get up to date information about the location of the file.
- 6 Records Management will operate file control procedures to ensure that the information recorded on the tracking system is kept up to date, and shows the correct location of the file. This will include regular prompts to the officer shown on the tracking system as having a file. Officers receiving such a reminder should return it as soon as they can, so that the information on the tracking system can be kept up to date for the benefit of their colleagues and themselves.

ELECTRONIC RECORDS, E-MAILS AND ELECTRONIC FAX MESSAGES

Purpose: *To explain the Agency's standard for managing electronic records, and to give you tips for best practice.*

- 1 The Head of Records Management must be informed of any new collections of electronic records, or changes to the format of electronic records, so that he can maintain an inventory of information systems and assets. He will decide whether or not the records are likely to have long-term value, or merit selection and transfer to the National Archives. He will have to make arrangements for those with long-term value to be preserved permanently, with sufficient metadata to enable the reader to be able to locate and read the record and understand it in context.

Electronic files (eRIK/Solcase)

- 2 Once the decision has been taken to begin creating and managing electronic files they will then become the Official Registered Files. For ease of use electronic filing systems will mirror the paper filing systems and use the same file references as the relevant paper files.
- 3 Shared areas on shared drives should be set up to enable groups with a specific shared responsibility or interest to file and access information that is held on registered files (or indeed for reference material). For OKS the g:\ drive should be used, and the filing structure should be set up using the following hierarchy:
g:\Division\Group\Team\file title\reference.
- 4 The 'print records to paper' policy will continue for non eRIK users. COCAD, European, GLS and DOCS should store all electronically created documents on eRIK and any related paper components within a paper file jacket. .
- 5 For this reason electronically produced documents, e-mails and faxes that record a decision or action, or add value to a decision or action, must continue to be printed to paper and placed on the Official Registered File to which they relate by the person with responsibility for maintaining the file.
- 6 Where access will be required for general reference across a team it must be stored on a shared area (drive), unless it is retained for personal reference. If work is held for personal reference IS can provide access in emergency on the authority of a senior manager. The information should be kept in structured folders (directories) according to subject

Scanning

- 7 Scanning of paper into an electronic system is not widely used in the Agency and will not be widely used in the foreseeable future. However scanners are available and are used for ease of reference of documents in voluminous

cases. Documents that have been scanned into an electronic system should not be destroyed, but should be placed on the registered file to which they relate.

E-mail and electronic fax messages

- 8 The following guidance refers to e-mail but it applies equally to electronic fax messages. It has been written from a records management perspective and complements the higher-level e-mail policy that has been written by Information Systems, which can be found in the Staff Handbook.
- 9 All information transmitted via e-mail across the Agency's network is considered to be the Agency's information and therefore a corporate information resource. It is also a public record under the terms of the Public Records Acts 1958 and 1967.
- 10 E-mail messages and electronic fax messages of value should be placed on the file to which they relate, by the person with responsibility for maintaining the file. If the file is held on paper they will be printed off and attached to it. The flow-chart at appendix 1 to Records Management Desk-note Number 3, will help you to decide where to file an e-mail message.

Sending messages

- 11 Make sure your document heading (subject line) clearly identifies what the document is about. This will help recipients judge the priority of your message and the need to view any attachment. Include the file reference.
- 12 Target your audience carefully. Do not send a message for information unless the recipient has a genuine need to know. It is easy to send messages to a multiple audience either by setting up groups or including users in the cc box, but this facility should be used as it would for a hard copy. If you would not have telephoned or sent them a paper copy, think carefully about their inclusion on that e-mail. E-mails to everyone at OKS cannot be sent without the approval of the Head of Information Systems.
- 13 Emoticons (common e-mail symbols) are not to be used. They are not widely understood, and are inappropriate for use in an official message. Only abbreviations that are commonly and widely understood should be used.

Receiving messages

- 14 If you are on leave for any length of time you must let someone else **access** your email, or divert it to a colleague. There is a facility that allows you to give proxy rights to other users so that they can access your e-mail in your absence.
- 15 If the message conveyed in the e-mail forms the basis of a decision which may need to be explained or justified at a later date it should be incorporated in the official registered filing system, whether that is paper or electronic, by either the sender or the recipient, whoever has the lead in the subject, and therefore has the official file. This will mean that the message is available to

all those who might need access to it, if the sender or recipient is away from the office.

Retention

- 16 E-mail is a public record, covered by the Public Records Acts 1958 and 1967.
- 17 E-mail messages will stay in your 'in-box' until you move or delete them. Just as with paper it is essential that messages are kept for as long as they are needed, but no longer. This is particularly important for e-mails which contain data about an identifiable individual because the Data Protection Act 1998 applies to these and keeping information for longer than it is needed is an offence under the Act. You can set up your e-mail to automatically delete or archive e-mail after a set time.
- 18 Similar conditions apply to information generated electronically, for example using MS Word or Excel. If electronic files are set up as convenience copies of records held in registered files the electronic file should be deleted a year after the file has been closed.

Security

- 19 If you receive and print e-mail containing protective marking up to RESTRICTED they should be treated in the same way as other RESTRICTED documents. More guidance is given under the heading SECURITY in the staff handbook.

PERSONAL AND TEAM REFERENCE MATERIAL

Purpose: *To explain the differences between reference material and material held on Registered Files, and to give you tips for managing the material so that it supports you.*

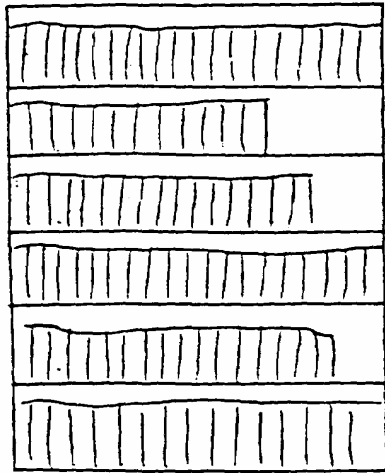
- 1 Collections of personal and team reference material will be distinctly different to Registered Files. They will be used primarily to hold information that has been sent to the user for information only, or in a matter in which they do not have the lead in the Agency, as opposed to material that records work they are responsible for (which would be held on a Registered File). For example it will include copies of circulars and guidance notes. These collections are less important to the user than registered files.
- 2 It pays to share reference material as much as possible, to save space and time in managing it and to avoid duplication. The risk of staff referring to out of date information will be reduced. Here are some tips for managing reference material:
 - be selective and concentrate on documents related to you and your responsibilities
 - label groups of material clearly and logically, divided into groups according to subject
 - file material on a particular subject in date order
 - review the collection regularly (every six months or more frequently in fast changing environments) and destroy material that is no longer useful.
 - have systems in place to replace advertising and product literature with the newest or updated version.
- 3 Responsibility for maintaining the collection of reference material could be assigned.
- 4 Guidance on the management of electronic collections of reference material can be found in Records Management Desk-note Number 10.

STORAGE OF PAPER RECORDS AND OPERATING THE CLEAR DESK POLICY

Purpose: To explain the Agency's clear desk policy, and to describe the benefits that could be realised when it is operated. It gives practical ups on implementing it and making best use of available storage space.

The clear desk policy

- 1 The Agency's clear desk policy ensures that information is kept securely, so that it is available only to those who have a legitimate need to see it for their work. The Agency has a duty to ensure that sensitive or personal information, which many of the Agency's files contain, is kept securely and in conditions where it is only available to those with a need to it, regardless of whether the information may become public knowledge. The need to operate a clear desk and screen policy has become critical with the introduction of the Data Protection Act, which requires that data about an identifiable living individual is kept securely.
- 2 It is not just about keeping information secure, but is about keeping it in well ordered and efficient filing systems, so that it can be found quickly when it is needed.
- 3 During the working day files are at risk from the idle curiosity of visitors. During non-working hours they are at risk from contractors and intruders. At any time there is a risk of fire or flood, which could have a devastating effect on the continuation of the Agency's business.
- 4 In addition to safeguarding the information there are very clear, and achievable, benefits to operating a clear desk policy:
 - a more ordered and pleasant working environment
 - improved efficiency (being able to find information quickly)
 - an improved image for visitors.
- 5 The policy is the aim of the Agency, and must be met by all staff as far as possible. However, in reality we are limited by the amount of storage space we have available, and even when we apply best practice in records management, we may have more to store than the space allows. The following hints and tips will help you to apply the clear desk policy.
- 6 Current (live) Registered Files should be stored as close as possible to the users. Registered files should never be stored in desk drawers where they are not available to other users.
- 7 Store files (and papers) in cupboards and filing cabinets laterally (i.e. On their spines). They will occupy less space than when stacked, and files can be removed and replaced more easily. The illustration below shows this.

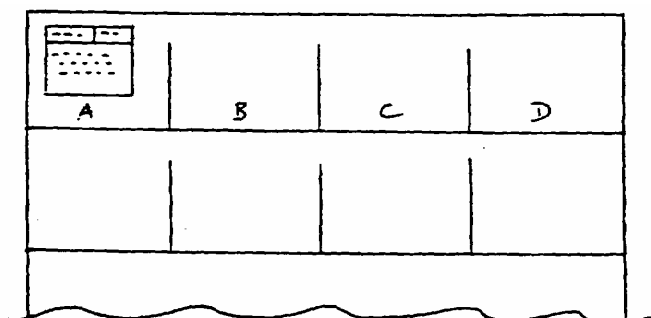


- 8 Files should be stored within each team in a standard order that has been agreed and accepted by all team members, such as reference order.
- 9 Here are some tips:
- team based filing is often more effective in terms of file management and use of storage space, than storing files in personal collections.
 - use collapsible folders rather than ring-binders.
 - do not store papers in boxes (such as Xerox). Unless full these waste space, and removing papers is a nuisance.
 - if files are stored in groups, other than in reference order, allow realistic space for them, do not allow more than they need.
 - give priority for the use of lockable cabinets to files rather than stationery supplies.
 - fit cupboards with the maximum number of shelves appropriate for files to be stored laterally.
 - share reference material (see separate desk-note for advice).
- 10 A good alternative to lockable cupboards is a lockable room, which could be used solely as a filing room for live files, if existing equipment (including open racking) is put into it. Provided files and paper are put into the room at the end of the day, and the door is locked the clear desk policy would be operated. This would remove the **need to lock all of the cupboards. However, such a system would require strict management, and would need effective procedures to work successfully.** Records Management would be happy to advise anyone wishing to set up a similar system.
- 11 Reference material can often be shared by all members of a team, when it is placed centrally in one collection. If it is shared, not only will less space be occupied, less time will be spent managing it and the risk of staff referring to out of date information will be reduced. Responsibility could be assigned for maintaining the collection.

Consider a managed random system

- 13 A managed random system for groups of larger files, and those with a great deal of supporting papers usually works better than the alternatives, such as filing by reference order. With a random storage system each cupboard is given an identifier, such as a number, and each shelf has a further identifier. When each shelf is divided into compartments a final identifier is needed. The

location of any file and related papers would be recorded on an index. The location would be a code showing the cupboard, shelf and compartment where these are stored. The illustration below shows this. The compartment with a file drawn into it in the illustration would be at location 1AA.



- 14 Papers in any one case would not need to be kept together. The tracking system would be the key to retrieval. The location assigned to a file would be its home until it is no longer kept in the office. The benefits of such a system are:
- better use of the available space (with no need to predict how much paper a case will generate)
 - re-organisation is unnecessary as files can fill any available space.

Choosing the best equipment

- 15 Cupboards with shelf dividers, rather than filing cabinets should be purchased every time, and cupboards with roller shutter doors are better than those with outward opening doors because the doors are less obtrusive, so less likely to cause accidents. The advantages of cupboards over filing cabinets are:
- a cupboard fitted with six shelves, each one metre wide holds at least double the measurement of files as a filing cabinet occupying the same floor area
 - all shelves can be accessed at one time, as opposed to one drawer at a time in a filing cabinet
 - drawers in filing cabinets often stick or break, making the drawer useless
 - access to contents of cupboards is easier for people of all heights.

Storage: Current File Store (CFS)

- 16 Current case papers up to and including the 'Confidential' security level, can be boxed up and stored within the on-site current file store. This should mean that there is no need to store boxes of papers around desks, within office spaces. During normal office hours, current case papers can be retrieved within 2 working hours. If papers are needed outside of normal office hours, they should be ordered in advance, so that the File Store team has the time to return them to you as and when needed.

For details on how to arrange a collection or request the delivery of Current File Store Boxes, please refer to the revised Current File Store Guidance Notes and Forms at [Appendix 9](#)

MANAGING INFORMATION PUBLISHED THROUGH OUR FREEDOM OF INFORMATION PUBLICATION SCHEME

Purpose: *This desk-note is aimed at owners of information published through the Agency's Freedom of Information Publication Scheme and sets out the Agency's policy for editing and managing it and for handling requests.*

1. Owners have been identified for all of the information published through our Freedom of Information (Fol) Publication Scheme. The Publication Scheme Register lists these owners and is maintained by Records Management.
2. The Freedom of Information (Fol) Publication Scheme can be viewed on our website <http://www.tsol.gov.uk/publications.htm>. It sets out information that we commit to publishing under the Freedom of Information Act 2000 (i.e. making available to the public, either proactively through our website or on request).
3. Owners are responsible for ensuring that all aspects of the policy set out in this guidance is followed in respect of the published information they own.

Managing published information

4. Published information should be managed in line with this policy, so that we can ensure that the right information is published and that the right version can be found quickly and easily when a request has been received.

Summary of guidance

5. The following is a summary of this guidance:
 - Edit information where appropriate before publishing (see 6-7 below)
 - Put published information on a registered file available from our Fol Officer (see 9–13 below)
 - Include a version number as a header in the top right hand corner of every published document (e.g. 'Version 1 – 21/10/02') (see 14-15 below)
 - Provide latest version of published information to website team, and tell them if it replaces a previous version (see 20 below)
 - Arrange for the nomination of a new owner if you move jobs and will no longer own the information (see 24 below)

- Convert published information to another format should existing software be about to become obsolete (see 25 below);

Editing information

6. Information published through our Publication Scheme may be edited or provided in summary form on the grounds of sensitivity or confidentiality, for example because it relates to security matters, or consists of advice given to our clients. This would mean removing sensitive or confidential information before publication, but leaving in information that is not sensitive or confidential.
7. The following non-statutory broad criteria are suggested as likely to warrant editing before information is published. Editing published information is largely a matter of common sense, and the application of these criteria is for individual judgement. The criteria suggested are not intended as an exhaustive list and there may be other criteria which we would want to apply. Additional exemptions came into force in January 2005, when the access provisions of the Act come into force:
 - Information in which a third party is named or from which they could be identified, where they have not given their consent to the information being published (this is required to meet the requirements of the Data Protection Act 1998);
 - Information that merits a Protective Marking (Restricted, Confidential, Secret or Top Secret), even if one has not been applied (see chapter 9 in the Staff Handbook for guidance on applying Protective Markings);
 - Commercially sensitive information, including any that might give our competitors a commercial advantage over us;
 - Details of our security arrangements, either ours or others;
 - Where it is considered that a claim of Legal Professional Privilege would be upheld.
8. Contact our FoI Officer if you would like advice on this issue.

Place published information in a registered paper file

9. Owners should place each individual class of published information that they own in a registered paper file that will be provided by our FoI Officer whenever a new class is created. The file will be given a title in the format 'Published Information - Title of the information as described in our Publication Scheme'.
10. The file will be registered in the series FOI, and our FoI Officer will maintain a database recording key details about the file and its location.

11. Owners should place a paper copy of the published information on the file as soon as they receive it, and complete the file contents index that will be inside the file. The version number (see below) should be included in the index.
12. Files should be stored securely in a place that is readily accessible to the owner and their colleagues in their absence.

Version control

13. Owners should include a version number as a header in the top right hand corner of every page of the published document, in the following example format as soon as it is ready for publication:
'Version 1 – 21/10/02, for the first version;
'Version 2 – 10/11/02, for the second version.
14. When a new version of the document is published it should be placed on the registered file holding the previous versions, and the file index should be updated.

Electronic versions

15. Published information that has been produced electronically should be maintained electronically by owners and saved into the appropriate file on the shared drive that has been set up for owners of published information at 'g:\foi\published information' or eRIK as appropriate (for OKS only). The file will be opened by the FoI Officer, and will mirror the paper file. The document should be indexed under the title by which it is known in our Publication Scheme, and should include the version number, as described above.

For example

*'List of the main Boards, Committees and Working Groups
inside the Department version 1 – 21/10/02'.*

Dealing with requests for published information

16. Requests for information included in our Scheme should be referred to the Agency's FoI Officer, who is responsible on a day-to-day basis for handling such requests. General FoI e-mail and postal addresses have been established and members of the public are directed to send any requests for published information to these. Our FoI Officer will deal with requests when they are received at these addresses.
17. Our FoI Officer will send the requester the latest version of the published information, taken from g:/foi/published information.
18. The Agency has to respond to requests made under the FoI Act within twenty days.

Information published on our website

19. We have committed to publish only the current version of published information on our website. Owners are responsible for supplying the latest version to the Information Services team that manages our website, and for telling them when a new version replaces a previous version.

Closing files

20. Files should be closed in January every year, by sending them to our FoI Officer, who will retain them for five years before review, in line with our retention policy for published information. Our FoI Officer will prompt the closure of files at the same time as issuing new ones for the next year.
21. Our FoI Officer will send closed files to the File Store for storage. These will be available to 'owners' by sending a request to the File Store in the usual way, as outlined in Records Management Manual Desk-note 9.

New owners of Information

22. If an existing owner of published information changes jobs and is no longer responsible for the information a new owner should be nominated from their work area. Our FoI Officer should be informed.

Obsolete software

23. In the event that published information is held on software that is about to become obsolete it should be converted to another format. Information Systems will warn us about such an event in advance.

Annual review of the Scheme

24. Our FoI Officer will prompt an annual review of our Publication Scheme, which will include asking the Executive Board if there is any additional information that we could commit to publishing.

Records of the handling of requests

25. Records of the handling of requests for published information will be placed on a registered file by our FoI Officer, so should not be placed in the file with the published information held by owners

REQUESTS FOR ACCESS TO INFORMATION

Purpose: *To explain the Agency's procedure for handling requests for information under the Data Protection Act 1998 (DPA), the Freedom of Information Act 2000 and the Environmental Information Regulations.*

1. People now have extensive rights to data and information which we hold. Handling their requests wrongly, or failing to recognise a request, can cause serious trouble. All requests described in this guidance should be passed to the Agency's Head of Records Management, who will also be able to help if you are not sure whether a formal request has been made.

This guidance explains the Agency's policies and procedures for handling requests for information under:

- The Data Protection Act 1998 (DPA)
- The Freedom of Information Act 2000 (FoIA) and
- The Environmental Information Regulations.

3. Such requests for information will generally come from members of the public, including journalists and companies.

Procedure

4. All requests received under the DPA, FoIA or EIRs must be forwarded promptly to the Agency's Head of Records Management, who is responsible for handling them. They will:
 - Consider whether there is any reason why the information requested should not be supplied and, if so, whether or not an exemption applies
 - Consult colleagues who hold the information and seek legal advice from COCAD, if necessary
 - If the information is to be disclosed, identify the appropriate format for providing the information, and
 - Respond appropriately to the requester
 - Keep colleagues who hold the information informed of progress.

Implications of failure to follow procedure

5. It is essential that this procedure is followed to ensure that our response is registered, appropriate, consistent and in line with any statutory or other relevant requirements. Failure to do so could result in:
 - The Agency being criticised publicly by the Information Commissioner (who is responsible for overseeing compliance with the DPA, the FoIA and the EIRs)
 - Enforcement action being taken by the Information Commissioner (including court action) for non-compliance with the DPA, the FoIA or the EIRs
 - Court action being taken by individuals under the DPA for information to be disclosed and/or compensation for damage.

Exclusions

6. The Agency receives many requests for information every day from those with whom we need to share information, for example from our clients, other parties in a case where the Agency is also a party, the courts, and from other government departments and bodies. This guidance is not likely to cover such requests but if you are in any doubt, please contact the Head of Records Management to discuss.

How to recognise a relevant request

7. It is not always obvious that a request is being made under the DPA, FoIA or EIRs, so here is a brief summary of the scope of each of these, to help you identify requests that need to be sent to the Head of Records Management. Once again, if you are in any doubt, contact them to discuss.

DPA

8. The DPA provides for individuals to request information held about themselves that is held by the electronically or in paper format. The individual is entitled to be informed as to whether or not the Agency does hold such information and, if so he or she is entitled to a description of the information, the purposes for which it is held and the persons to whom the information is, or may be, disclosed. The individual must be supplied with the information in an intelligible and permanent form unless an exemption applies. There is an obligation on the Agency to reply to requests for information under the DPA promptly but in any event within 40 days of receipt.

FoIA

9. The FoIA provides a general right of access to all recorded information held by public authorities, which includes central and local government, other public bodies and organisations such as schools and the Health Service. On 1st January 2005, section 1 of the FoIA gave the public the right to request information held by public authorities.
10. However, from 30 November 2002, central government departments and agencies were required to have publication schemes in place. Our scheme was submitted to the Information Commissioner for approval. It set out the information that we commit to make available to the public. It appears on our website and is on our intranet. Requests for information included in our Scheme should be referred to the Head of Records Management who is responsible on a day-to-day basis for handling such requests. The Agency is required to respond to requests made under the FoIA within twenty days.

EIRs

11. A request may ask for information relating to where the Agency obtains its furniture and paper, and whether these have been obtained from sustainable sources.

See [Appendix 10](#) for the Agency's Code of Practice for Data Protection

RECORDS MANAGEMENT PROCEDURES FOR THE PRIVATE OFFICE

Purpose: *Sets out the records management procedures for the Private Office.*

- 1 These procedures have been produced in the light of generic guidance that was issued by the Cabinet Office on 10 April 2001 about the management of Private Office records. That guidance was based on the requirement that good records management procedures within Private Offices are necessary to:
 - Meet statutory obligations, placed upon government departments by the Public Records Acts 1958 and 1967 and other relevant statutory and non statutory requirements, including the Data Protection Act 1998, the Freedom of Information Act 2000 and the Environmental Information Regulations
 - Enable departments to produce as evidence to inquiries, original paper submissions to Ministers and Permanent Secretaries, including any annotations they may have made
 - Reduce the risks associated with litigation by making it easier to identify and retrieve relevant information
 - Ensure accountability and provide an audit trail, which relays the views of the Minister or Permanent Secretary to the relevant business area
 - Protect information, which is a valuable resource.
- 2 The Cabinet Office guidance suggested two models that private offices could adopt. In summary these were:
 - Few records would be retained by the Private Office, and instead submissions and other papers would be sent back to the civil servant with responsibility for the case or subject, with annotations by the Minister or Permanent Secretary
 - The Private Office would retain records referred and generated to the Minister or Permanent secretary in registered subject files.
- 3 The Private Office, in agreement with Records Management, decided that the second option best suited the way they work, and the Agency's current records management arrangements. These procedures have been agreed between the Head of Records Management and the Private Office.
- 4 These procedures meet the Agency's Standard for Records Management, which is set out in the Records Management Manual, where further guidance about records management and surrounding legislation can be found. All staff have a copy of the manual.

Registered Files

- 5 Registered files are used to store papers received and generated by the Private Office. The Private Office opens these.

File Title

- 6 Each file should be given a meaningful title that accurately describes the subject of the contents of the file. Non-specific or generic terms, such as 'general correspondence' or 'miscellaneous' should be avoided, because these will effectively become dustbins, and retrieval of records about any one subject will be difficult. Acronyms and abbreviations used in the title should be those in common use, otherwise the words should be written in full.
- 7 A new file, or series of files, should be opened each year for matters that are likely to continue indefinitely.

File Reference

- 8 Each file is allocated a reference, consisting of the following elements:
 - A prefix 'PO', to indicate that it relates to the Private Office series of files;
 - The year of registration in a four digit form, for example '2002';
 - A number allocated to the files consecutively, which makes the reference unique
 - The part number, for example 1, for the first file registered under a reference.
- 9 To illustrate this, the first file registered in 2002, would have the reference 'PO/2002/1/1', and the 100th file registered that year would have the reference 'PO/2002/100/1'. When a continuation file is opened under that reference it would be 'PO/2002/100/2', and so on.

File List

- 10 Registered files are recorded on a list, which is maintained on MS Word, and which acts as a database for text retrieval. The following details about a file should be recorded on the list:
 - Title
 - Reference (in the format described at 2.4)
 - Location, in the format 'PO', for Private Office, 'PR' for Paper Room, D for destroyed.

Electronic Records

- 11 Emails and documents produced electronically should be stored on eRIK.

File Storage

- 12 Registered files in live matters are stored in alphabetical order, according to the first letter of the key word in the title (usually the first word).
- 13 The filing cabinets contain the latest part file opened, or the part 1 file, if that is all there is. The cupboard holds the previous part file for all live matters.

Closing and Sending Files to the File Store

- 14 Registered files should be sent to the File Store for storage, once they are no longer need regularly for reference by the Private Office.
- 15 The location on the file list should currently be changed to 'PR'.

Retrieving Files from the File Store

- 16 Files can be retrieved from the File Store by sending an e-mail to 'paper room', with details of the reference and title of the file requested. The File Store will deliver the file within half a working day.
- 17 The file list should be updated to show the location as 'PO'.

Retention Periods

- 18 Records Management will assign an appropriate retention period to the file when it is received for storage, in line with the schedule set out at *appendix 11*. The retention period will run from the date of last action physically recorded on the file. This schedule has been agreed between the Private Office and the Head of Records Management. Changes should be made only with the agreement of both parties.
- 19 Records Management will review the files after the appropriate retention period has passed, and will select those worthy of further retention or with potential for permanent preservation at the National Archives. They will send the Private Office a list of any files they recommend for destruction, and will only destroy files with the agreement of the Private Office. The Private Office should return the list to Records Management, annotated with 'retain' for files needed for longer, or 'destroy'.
- 20 The file list should be updated to show the new status 'D', for all files that have been destroyed.
- 21 Other records included in the retention schedule are: Permanent Secretaries' official diaries; declined invitations; Permanent Secretary's notebooks, Private Secretary's notebooks.

File Security

- 22 Files containing documents with a Protective Marking (Restricted, Confidential, Secret or Top Secret) should be protected and handled appropriately, in line with the guidance set out in the Staff Handbook.

THE MANAGEMENT OF PUBLIC INQUIRY RECORDS AND OTHER TEMPORARY BODIES

Purpose: *To set out the Agency's policy for managing records generated in the course of our involvement in Public Inquiries and the work of other temporary bodies, which have been set up to investigate or provide advice or recommendations on a particular issue or event.*

- 1 This guidance has been adapted from generic guidance produced by the National Archives, and it draws heavily on that guidance.
- 2 Good records management procedures within temporary bodies are necessary to:
 - Make available to the body accurate and reliable records to enable it to complete its brief or meet its terms of reference, including the provision of a final report
 - Ensure that records can be readily retrieved when required
 - Ensure accountability and provide an audit trail
 - Meet statutory obligations of the Public Records Acts 1958 and 1967, the Data Protection Act 1998, the Freedom of Information Act 2000 and other legislation
 - Keep information which will facilitate authentic reconstruction of the record keeping system
 - Keep records in a way that allows them to be identified for historical and research purposes.
- 3 It is the responsibility of the department that is sponsoring the Public Inquiry or temporary body to ensure that:
 - Effective records management procedures are established for the management of records generated by the Inquiry or body from the outset
 - Such records are safeguarded
 - Such records are appraised and disposed of in accordance with current legislation and guidance
 - Advise the staff of the Inquiry or body adequately on records management issues.

The Agency's role

- 4 It is more likely that the Agency will act as secretary to the Public Inquiry of temporary body, than sponsor it. So, if for example the sponsor is the Department of Health, then that department is responsible for establishing records management procedures and 'owns' the records.
- 5 The secretary is responsible for:
 - Informing the Departmental Record Officer (DRO) of the sponsoring department of the existence of the Inquiry or body, or informing the Head of Records Management Department at the National Archives if there is no sponsoring department (contact details available from the

Agency's Head of Records Management), and, where the Agency is providing the secretary, for informing the Agency's Head of Records Management

- Agreeing the records management policies and procedures with the DRO of the sponsoring department (or TNA)
- Ensuring that the records of the Inquiry or body are maintained during its existence in such a way that the requirements detailed at 2 above are met
- Ensuring that staff are made fully aware of the need to safeguard and maintain adequate records
- Arranging early discussion with the DRO of the sponsoring department, TNA about the terms of reference of the Inquiry or body, with a view to determining those records which are likely to have long term value, and also with the Agency's Head of Records Management in cases where we are providing the secretary;
- Establishing a formal publication scheme within the terms of the Freedom of Information Act 2000 is drawn up, or if the sponsoring department already has a scheme, arranging for an amendment to be inserted in that scheme;
- Giving TNA and the DRO of the sponsoring department adequate notice of the winding up of the Inquiry or body so that appropriate arrangements for its records can be made;
- Making sure that members are made fully aware that the records of the temporary body are official and must not be removed from its custody.

Records generated by the Agency

- 6 The Agency will generate records as a result of its involvement in Inquiries or temporary bodies, and these should be managed in the usual way in line with the Agency's records management policies set out in this Manual, within a registered file.
- 7 The Agency's Head of Records Management should be involved in discussions about the retention of records generated by the Agency. Where the records are identified as requiring preservation at TNA as part of the records of the Inquiry or body they should be transferred with the Inquiry or body's records to TNA.
- 8 All other records should be destroyed in line with the Agency's retention policy when they have no further value.

Further guidance

- 9 Guidance specifically about establishing records management policies and systems, and retention of records for Public Inquiries and temporary bodies can be found in TNA's generic guidance titled 'Management of records of temporary bodies', which is available from TNA's website www.nationalarchives.gov.uk or from the Agency's Head of Records Management.

THE MANAGEMENT OF SPECIAL AND ORDINARY SHARE CERTIFICATES

Purpose: To set out the Agency's policy for managing special and ordinary share certificates

On Receipt at OKS

- Registry EO to be contacted immediately on receipt of the Share Certificate at OKS so that it can be logged on the Strong Room database showing its location (as described below).
- Share Certificates to be stored securely in a safe whilst with a division
- Share Certificates never to be placed on registered files
- Registry EO to be contacted to arrange collection by hand when any necessary work has been completed and the Certificate is no longer needed by the Division
- All Share Certificates to be stored in the Strong Room at OKS, and never with an off-site storage provider.

Logging Share Certificates Received

All Share Certificates to be logged on Strong Room database as soon as they are received, with the following details:

- Share Type: Special or Ordinary
- Name of company in which shares are held
- Name of the client for whom the shares are held
- Location of the Share Certificate in Strong Room (row, bay, shelf)
- Location if on loan (Name of TSol person Share Certificate loaned to)
- Date due for return to Strong Room (two weeks after loan, and then updated each time an extension has been approved, see below).

Retrieval for Loan

- Share Certificates will only be sent to TSol staff
- Change location of Share Certificate on database
- Attach covering note, seeking signed receipt by borrower and asking the borrower to contact the Registry EO when the Share Certificate is ready for return
- Take Share Certificate by hand to borrower
- Registry EO to file signed receipt in folder recorded on Strong Room database named 'Special Share Certificate Loans' and held in Strong Room.

Managing Loaned Share Certificates

- Telephone borrower to seek return of Share Certificate
- Collect it if they have finished with it

- Give them two more weeks (or another period agreed with them), and update the 'Date due for return to the Strong Room'

Returning loaned Share Certificates to Storage

- Collect the Share Certificate by hand
- Update the location details on the database
- Remove the 'Date due for return'
- File the Share Certificate in its designated place in the Strong Room.

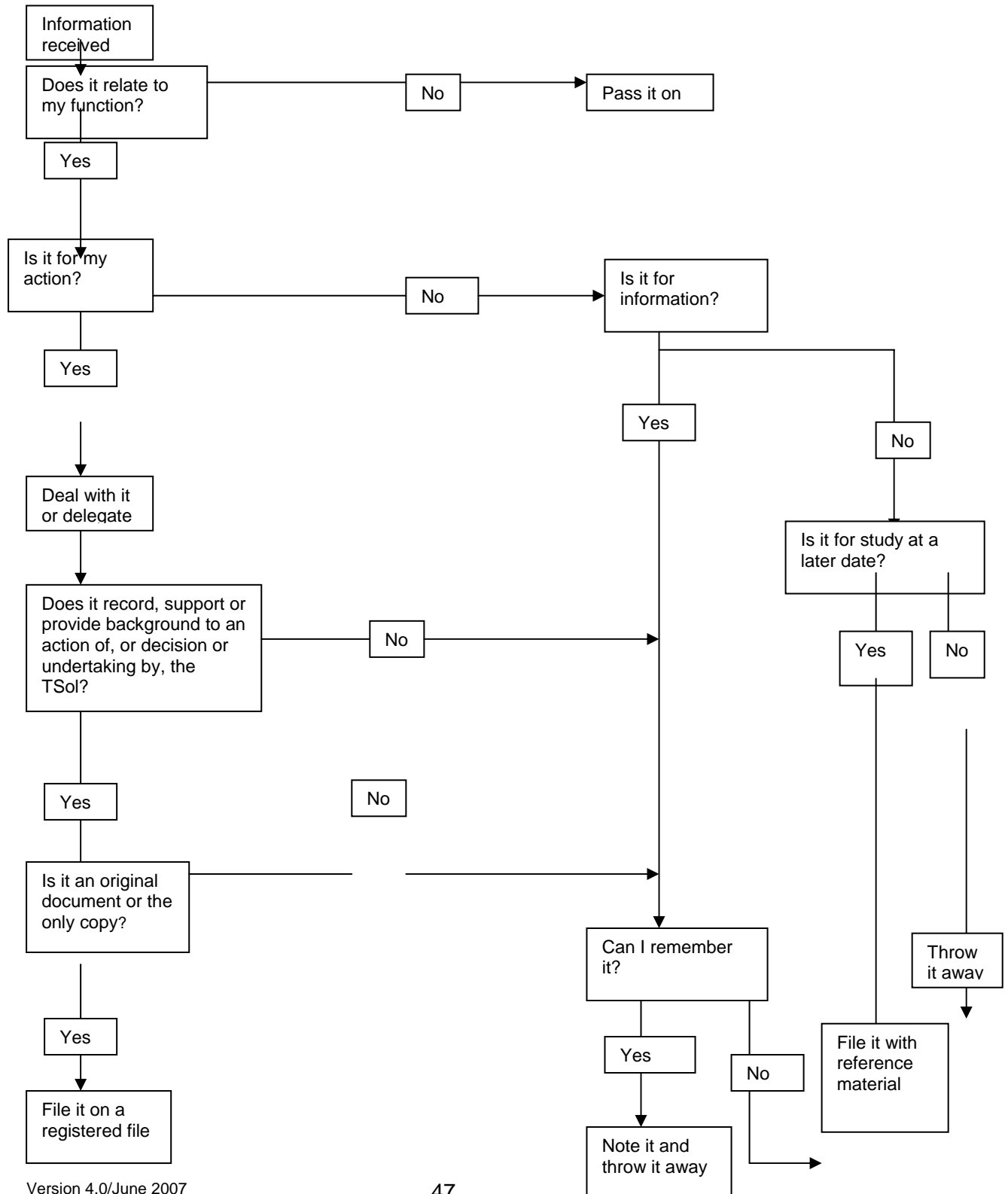
Auditing Share Certificate Holdings

- Registry EO to audit Strong Room database records in respect of Share Certificates annually to confirm location of all that are held on the database and which are recorded as with TSol
- Registry EO to obtain list of all shares from which TSol has received a dividend from Finance, and compare these to the shares recorded on the database. Then to locate those that have not been recorded on the database by contacting the appropriate Divisional Head.

Appendices

Appendix 1 - Deciding what to do with new information - flow chart

DECIDING WHAT TO DO WITH NEW INFORMATION



Appendix 2 - Request to open a new file

REQUEST FOR A NEW REGISTERED CASE JACKET

Complete the following table for a new case or matter in which no registered file exists.

File Title/Name of case	
Category (see retention schedule)	
Client department	
Client's reference	
Name of contact	
Contact address	
Contact Unit	
Team	
Manager's name	
Case Holder's name	

Please complete this form and email to Records and Registry

The completed file jacket will be sent to you via internal/external mail.

The Registry can be contacted on **0207 210 3077** with any queries.

NAME: _____

ZONE: _____

EXT: _____

DATE: _____

REQUEST FOR A NEW PART CASE JACKET

Complete the following table for a continuation/part file.

Only use this form for a case or matter for which a file has already been registered.

File reference	
File name	
Continuation/part number	

If you would like registry to ring you immediately with a reference number tick here

The completed new part jacket will be sent to you via internal/external mail.

The registry can be contacted via **email** to **Records and Registry** or via telephone on **0207 210 3077** with any queries.

NAME **ZONE** **EXT** **DATE**

Appendix 3 - Standard prefixes in use in the Agency

PREFIXES IN USE IN THE AGENCY

The following is a list of registration prefixes in use in the Agency, showing the users:

Prefix	Used for	Used by
A Divisions	Advisory work on files registered up to 31/12/1999	Advisory
AD Divisions	Advisory work on files registered since 1/1/2000	Advisory
B Division	Management of European Division	European
BS	Business Strategy Unit	DOCS
BV Vacantia	Bona Vacantia work	Bona
C	Conveyancing	GPL
CP	Contracts & Procurement	DOCS
E Division	European work on files registered up to 31/12/1999	European
EU Division	European work on files registered since 1/1/2000	European
G Division	Costs related files	Litigation
IS	Information Services	DOCS
L Division	Litigation work on files registered up to 31/12/1999	Litigation
LA	Non-casework related papers from 01/07/05	Litigation A
LT Division	Litigation work on files registered since 1/1/2000	Litigation
MT B2	Litigation B2 registered files from 1/10/2002	Litigation
NT D2	Litigation D2 registered files from 1/10/2002	Litigation
PO Office	Private Office registered files	Private

PT C2	Litigation C2 registered files from 1/10/2002	Litigation
Q Division	Queens Proctor cases	Any
RM	Records Management	DOCS

Appendix 5 - Record of Disbursement (Finance Certification)

TREASURY SOLICITOR LITIGATION DIVISION
RECORD OF DISBURSEMENTS

Description	£	Date PRF sent to Finance	Description	£	Date PRF sent to Finance Branch
Court Fees			Medicals & Experts		
Counsel's Fees			Travel and Subsistence		
Counsel's Fees			Miscellaneous		

Appendix 6.1 - Retention schedules for Advisory, Bona Vacantia and DOCS

Retention Schedules

Advisory Division		
Type of Registered Papers	Standard Retention Period (in years)	Comments
Papers of short -term interest	5	
Advice on matters of long term importance including Policy or Major Legislation	10 to 5	Papers which may be of interest to the National Archives should be identified by a note inside the file cover.

Bona Vacantia Division			
Category	Type of Case	Standard Retention Period (in years)	Comments
A	SRA (Estates)	5 Years	Period run from the date of latest correspondence
B	Freehold / Leasehold Property (Estates)	Kin admitted - 5 years No kin found: Correspondence 12 years Accounts etc 30 years	5 years run from the date of latest correspondence
			12 and 30 years run from the date of death
			At the 12-year review, File Store staff will remove from the file cover all documents on the right-hand side of the file, and return the file to the shelf to await second review in a further 18 years
	Before archiving, case holders should ensure that all documents necessary for accounting to kin are tagged onto the left-hand side of the file cover		
C	Net Estate over £5,000	As B above	As B above
D	Net Estate Less than £5,000	As B above	As B above
E1	Bank and Other Cash Balances (Companies)	5	Period to run from date of latest correspondence.
E2	Intellectual	5	As E1 above.

	Property (Companies)		
E3	Land Charges, Mortgages, Shares (Companies)	5 years if no land unsold; 20 years if land unsold	5 years to run from date of last correspondence
			20 years to run from date of dissolution (subject to a minimum of 5 years from date of last correspondence)
E4	Freehold Reversions	5 years if no land unsold; 20 years if land unsold	
E5	Other Land (Companies)	5 years if no land unsold; 20 years if land unsold	
Bona Vacantia Division cont'			
Category	Type of Case	Standard Retention Period (in years)	Comments
E6	Pension Schemes	5	Period to run from date of latest correspondence
E7	Miscellaneous	5 years if no land unsold; 20 years if land unsold	
G	General File	Refer to Head of Division	
H	SRA (Companies)	5	Period to run from date of latest correspondence
NC	Northern Ireland (Companies)	5	Period runs from date of dissolution
NE	Northern Ireland (Estates)	5	Period runs from date of death
Q	Query	5	Period to run from the date of the latest correspondence
R	BV Registry Queries (Estates)	1	These are now kept in the BV Registry
V	BV Registry Queries (Companies)	1	These are now kept in BV Registry
Z	Property Conveyancing	5 years, or 30 years if TSol has made an acquisition	Periods run from the date of relevant deed (e.g. transfer) or, if TSol has granted a lease, from the expiry of the term
			The case holder should note the retention period on the front of the file before closure, together with the date of the deed or transaction from which the period is to run

DOCS Division	
Human Resources	
Category	Retention Period / Comments
V Series Files	To be reviewed annually.
Personal Files of Established Staff	To be retained until 85 years after the employee's date of birth or 5 years from the date of death, whichever is the later.
Personal Files of Un-Established Staff	The Record of Service, Official Secrets Act declaration and any papers relating to injury on duty to be retained as above, but all other papers need only to be retained until 15 years from the date of leaving the service.
Finance	
Category	Retention/ Comments
Law Charges Account –Registers & Vouchers	6 years
Law Charges Account – General Ledgers	12 years
Law Charges Account – Pay Files	To be retained with Personal Files by Establishments Branch
Crown Nominee Account – General Ledgers, Registers and Vouchers	12 years
Crown Nominee Account – Estate Accounts	To be microfilmed and preserved
Trust Fund Accounts	To be retained until Trust is terminated, then preserved by TNA

I confirm that for the matter held under:		Tick
File Reference		
1	No further action is expected on the case	
2	All incoming/outgoing, external/internal communications have been answered and dealt with.	
3	No outstanding money is due from or to the other side.	
4	The client monies account for the file is clear – check with the Client Monies Team.	
5	All fees due to solicitor agents, counsel, experts, etc have been authorised and passed to Finance for payment – check with the Payments Team that no invoices received are unpaid.	
6	I have considered whether there are any reasons why this file should not be retained for the standard period set out in the Agency's retention schedule, and taken appropriate action.	
7	I am not retaining any continuation/part file under this reference, and they can all be closed and put into storage	
8	Either: Accompanying papers have been removed from ring binders and placed into bundles for storage, or there are no papers outside of the file jacket.	
9	All costs and/or compensation information has been passed to the Admin Team (Adverse Costs inc VAT, Costs recovered from the other side, Compensation paid and Case Outcome)	

Appendix 6.2 - Retention schedules for Litigation, COCAD & ECCG

Litigation File Plan Numeric Version

Litigation, COCAD & ECCG File Plan

DATIX Case Types		
Code	Title	Retention Period
1	AG ADVOCATE TO COURT(EXC QP)	5
2	HOME JR APPEALS EX MAGISTRATES	5
3	TOWN AND COUNTRY PLANNING AND COMPULSORY PURCHASE MATTERS (OTHER THAN PLANNING AND ROAD INQUIRIES)	5
3A	PLANNING-T&CP ACT 1990 S288	5
3B	PLANNING T&CP ACT 1990 S289	5
3C	PLANNING ACQ.LAND ACT 1981 CPO	5
3D	JUDICIAL REVIEW (PLANNING)	5
3E	WILDLIFE & COUNTRYSIDE ACT1981	5
3F	PLANNING T&CP ACT 1990 S287	5
4	ARBITRATIONS, BUILDING CONTRACTS AND OFFICIAL REFEREE <i>(*The 15 year period is to cope with possible claims of latent defect, to be considered on a case-by-case basis by the case officer)</i>	6 TO 15*
6	AG-REPORT ON PRIVATE BILLS	10
8	CHANCERY (MISCELLANEOUS) (for genuinely miscellaneous cases only)	10
9	COMMONS REGISTRATION AND FOOTPATHS	10
10	CONSUMER CREDIT	5 to 25
10A	CONSUMER PROTECTION	15
10B	COMPETITION APPEAL TRIBUNAL	15
10C	COMPETITION ACT 1998 WARRANTS	15
11	AG - CONTEMPT OF COURT	5
12	HOME JR COURT MARTIAL APPEALS	5
13	CRIMINAL INJURIES O'SEAS COMP	6
14	DAMAGED & LOST PROPERTY CLAIMS	3
15	DEBTS [EXC CARRIER'S LIABILITY	3
15C	DEBTS: CARRIERS LIABILITY	3
15C	HOME JR CARRIERS LIABILITY	3
15D	PROP DAMAGE/LOW FLYING PLANES	6
15E	OTHER PROPERTY DAMAGE	6
15F	ECONOMIC LOSS LOW FLYING PLANE	6
15G	OTHER ECONOMIC LOSS	6
16	DEFAMATION	6

17	DRIVING TEST APPEALS UNDER ROAD TRAFFIC ACT 1972	5
19	EUROPEAN CONVENTION [ECHR]	10
20	EUROPEAN COURT	2, 5 or 10
23	IMMIGRATION	3
23A	EXTRADITION/HABEAS CORPUS	5
23B	IMMIGRATION SERVICES COMMISSIONER	5
23B	TRIBUNAL-IMMIG SERVICES	5
23C	IMMIG JR-THIRD COUNTRY	3
23D	IMMI-JR/NASS/ASYLUM SUPPORT	3
23E	IMMI-JR/S94 CERTIFICATION NSA	3
23F	IMMI-CRT OF APPEAL-3RD COUNTRY	3
23H	IMMI SPECIAL IMMI APPEAL COMM.	3
23J	IMMI - FAMILY	3
23K	IMMI - IAA HEARING	3
23L	IMMI - IAT HEARING	3
23M	CIVIL PENALTIES	6
23N	IMMI - Other Judicial Review	3
23P	IMMI - Work Permits	3
23R	IMMI - EC/ECAA	3
23T	IMMI-JR-SECTION 55 NASS	3
23U	IMMI-JR NASS/EU ACCESSION NATS	3
24A	RELIGIOUS DISCRIMINATION	6
24B	EQUAL PAY	6
24D	DISABILITY DISCRIMINATION	6
24E	PENSIONS	6
24F	TERMS OF EMPLOYMENT	6
24G	APPOINTMENTS	6
24H	HOLIDAY/MATERNITY PAY CLAIM	6
24J	REDUNDANCY	6
24K	TUPE	6
24M	WORKING TIME	6
24N	NON-STANDARD CASEWORK	6
24P	TRIBUNAL PENSIONS APPEAL	5
24R	RACE DISCRIMINATION	6
24S	SEX/GENDER DISCRIMINATION	6
24T	TRADE UNION ACTION	6
24U	UNFAIR/WRONGFUL DISMISSAL	6
24V	PENSIONS	6
24W	WAGES CLAIM	6

Code	Title	Retention Period
24X	ASSAULT(GENERAL)	6
24Y	ASSAULT(SEXUAL)	6
25	INQUESTS	5
26	JUDICIAL REVIEW OTHER THAN PLANNING AND IMMIGRATION	5
26A	HOME JR PRISON SERVICE	5
26C	HOME JR PAROLE BOARD	5
26D	HOME JR CROWN PROSECUTION	5
26E	HOME JR MAGISTRATES COURTS	5
26F	HOME JR CICAP	5
26G	HOME JR CICA	5
26H	HOME JR AG EXC.ADVO/CONTEMPT	5
26K	HOME JR MUTUAL LEGAL ASSISTNCE	5
26R	JR NOT ELSEWHERE SPECIFIED	5
26S	I/VENTIONS-D. INCOMPATIBILITY	5
26T	PRISON DISCIPLINE HEAR (REP)	5
26U	PAROLE BOARD HEARINGS (REP)	5
26V	MALADMINISTRATION	5
26W	THIRD PARTY DISCLOSURE	5
27	COMP.PURCHASE & COMPENSATION	4
27A	EMPLOYMENT ADVICE	6
27B	ADVICE BY LITIGATION TEAM	5
28	AG FAMILY LAW ACT 1986	15 / Perm
28A	AG INHERITANCE ACT 1975	15 / Perm
28Q	AG QUEENS PROCTOR	15 / Perm
29	LETTERS OF REQUEST	5
29A	ASSAULT - INMATE ON OFFICER	6
29B	ASSAULT - INMATE ON INMATE	6
29C	ASSAULT - OFFICER ON INMATE	6
29D	ASSAULT - CONTROL & RESTRAINT	6
30	MONOPOLIES AND MERGERS	Permanent
31	PATENT	10
32	PERSONAL INJURY CASES (<i>*Asbestosis/MID cases – 30 years</i>)	6/30/60*
32E	ASBESTOS RELATED	30
32G	IND DISEASES - REYNAUDS	6
32H	INDUST'NOISE INDUCED DEAFNESS	6
32K	CLINICAL NEGLIGENCE	6
32L	CLIN NEG CNSENT/INFRMD CNSENT	6

32M	CLIN NEG FAILURE TO DIAGNOSE	6
32N	CLIN NEG PROV WRONG TREATMENT	6
32P	CLIN NEG FAILURE TO TREAT	6
33	RESTORATION	3
34	POSSESSIONS [EXC SQUATTER/L&T]	3
35	PROBATE	10
36	PROSECUTIONS	5
37	PUBLIC INQUIRIES (OTHER THAN ROAD AND PLANNING)	10
37A	PUB.INQ. WITNESS TO INQUIRY	5
37B	PUB.INQ-SERVICING INQUIRIES	5
37C	INQUIRIES - OTHER	5
38	PUBLIC INTEREST IMMUNITY	10
41	TRIB RENT ASSESSMENT	5
42	REPRESENT'N OFFICIAL RECEIVER	5
43	RESTRICTIVE TRADE PRACTICES	Permanent
44	ROAD & PLANNING ENQUIRIES	10
45	SHIPPING	10
46A	SQUATTERS	3 or 8
46B	TRESPASS	3 or 8
46C	NUISANCE	3 or 8
46D	LAND REG OTHER THAN 1925 ACT	10
46E	LAND DISPUTES	10
48	VESTING ORDERS IN CHANCERY	10
49	AG - VEXATIOUS LITIGANTS	50
49A	HABEAS CORPUS	3
51	BOARD OF VISITORS/REPRESENTATION OF PRISON GOVERNORS	5
53	LANDLORD & TENANT	5
53A	LANDLORD AND TENANT ACTS CASES	5
53B	PROPERTY TITLE	5
54	CHARITY	Individual
54A	CHARITY DIRECTIONS/SIGN MANUAL	Individual
54B	CHARITY REQUESTS S32 1993 ACT	Individual
54C	CHARITY APPLICATIONS UNDER S16	Individual
54D	CHARITY EX-GRATIA PYMTS/WAIVER	Individual
54E	CHARITY PROCEEDINGS(EXC BEDDOE)	Individual
54F	CHARITY BEDDOE APPLICATIONS	Individual
54G	CHARITY ACTIONS BY AG	Individual
54H	CHARITY ACTIONS FOR COMMISSION	Individual

Code	Title	Retention Period
54J	CHARITY CONSTRUCT CLAIMS (PT8)	Individual
54K	CHARITY APPEALS AGAINST ORDERS	Individual
54L	CHARITY WINDING UP UNDER S63	Individual
54M	CHARITIES DISPUTES	Individual
55A	DISQUAL DIRS/LIQUIDATORS (S.6)	5 to 15
55B	DISQUAL DIRS/LIQUIDATORS (S.8)	5 to 15
56	PEERAGES	Perm
57	BREACH OF CONFIDENCE	10
58	TRIBUNALS (NOT RENT)	7
58A	FINANCIAL SERVICES TRIBUNALS	7
58B	TRIB INSOLVENCY PRACTITIONERS	7
58C	TRIB MENTAL HEALTH	7
58D	TRIBUNAL INDEPENDENT SCHOOLS	7
58E	TRIB SPECIAL EDUCATIONAL NEEDS	7
58F	TRIBUNAL CARE STANDARDS	7
58G	TRIB PROSCRIBED ORG. APPEAL	7
58H	TRIB-APPEALS EX TRAFFIC COMM.	7
58J	SPECIAL ADVOCATES-SIAC & POAC	7
58K	INFORMATION TRIBUNIAL	7
58L	TRIBUNALS - OTHER	7
58M	STATUTORY APPEALS	7
58N	WITNESS SUMMONSES	5
59	SUPERVISION OF COMPANIES	7
59A	PROV LIQUIDATORS/WINDING-UP	7
59B	INSURANCE	7
60	BANKS, BUILDING SOCIETIES, FRIENDLY SOCIETIES	7
61A	CONTRACT-BUILDING/CONSTRUCTION	7
61B	CONTRACT-WEAPONS PROCUREMENT	7
61C	CONTRACT-INFO.TECHNOLOGY	7
61D	CONTRACT-INTELL.PPTY RIGHTS	7
61E	CONTRACT-TUPE	7
61F	CONTRACT FACILITIES /ESTATES MANAGEMENT	7
61G	CONTRACT - OTHER GOODS	7
61H	CONTRACT - OTHER SERVICES	7
62	HOME GP DISCLOSURE	5
63	HOME/JR DISCIPLINE-POLICE&HMPS	6
63A	MOD POLICE DISCIPLINE	6
64	FALSE IMPRISONMENT/MALICIOUS PROSECUTION	6

64A	FALSE IMPRISONMENT	6
64B	MALICIOUS PROSECUTION	6
64C	FALSE IMPRISON BY PRISON	6
64D	FALSE IMPRISON BY IMMIG SERV	6
64E	FALSE IMPRISON BY PROBATION SERV	6
64F	FALSE IMPRISON BY LICENCE	6
64G	FALSE IMPRISON OVERSTAY SENTCE	6
64H	FATAL ACCIDENT	6
64J	BREACH OF PRIVACY	6
64K	DENIAL OF RIGHTS	6
64M	ATTEMPTED SUICIDE	6
65	LAND REGISTRATION ACT 1925	10
66	HOME JR JUDIC/COURT OFFICIALS	5
70A	COCAD - ADVISORY WORK	5
70B	COCAD - COORD AND SECRETARIAL	5
70C	COCAD - LIAISON WITH THE GLS	5
70D	COCAD - LITIGATION WORK	5
70E	COCAD - PARLIAMENTARY BILLS WK	5
70F	COCAD - STAT INSTRUMENTS PREP	5
75A	ECCG - CENTRE OF EXCELLENCE	6
75B	ECCG - DISPUTES	6
75C	ECCG - PROC OF EXTNL LAWYERS	6
75D	ECCG - PFI	6
75E	ECCG - PUBLIC LAW	6
75F	ECCG - PUB/PRIV P'SHPS (PPP)	6
75G	ECCG - TRADITIONAL PROCUREMENT	6
75H	ECCG - OTHER	6
80A	MISFEASANCE IN PUB. OFFICE	10
80B	BREACH OF DATA PROTECTION ACT	10
80C	DAMAGES-HUMAN RIGHTS ACT 1998	10
80D	NEGLIGENCE (NOT LEADING TO PI)	10
80E	MOD ASSAULT COURSE	6
81	ABSEILING - PI	6
81A	AIRCRAFT ACCIDENT PI	6
81B	AIRCRAFT LOW FLYING PI	6
Code	Title	Retention Period
81C	BULLYING	6
81E	DIVING P1	6
81F	DROWNING PI	6

81G	ELECTROCUTION PI	6
81H	EXPOSURE/HOT/CLD/SUN/CHEMICALS	6
81J	FIRE (BURNS)	6
81K	FIREARM INJURIES	6
81M	SPRAINS/BACK (MANUAL HANDLING)	6
81N	NATO STATUS OF FORCES CLAIMS	6
81P	ORDNANCE(UNEXPLODED)	6
81Q	PARACHUTING PI	6
81R	POISONING (FUMES)	6
81S	POISONING (LIQUIDS)	6
81T	POISONING (SOLIDS)	6
81U	PSYCHIATRIC PI	6
81V	PTSD	6
81W	RADIATION P1	60
81X	ROAD TRAFFIC ACCIDENT PI	6
81Y	SPORTING INJURY PI	6
82	IND DISEASE STRESS AT WORK	6
82A	TRAINING AREA PI	6
82B	TRIPPER/SLIPPER	6
82C	VIBRATION WHITE FINGER	6
82D	RAIL CRASH	6
82E	CLIMBING (MOUNTAINEERING)	6
82F	EMPLOYER LIAB ACCDNT AT WRK	6
82G	OCCUPIER'S LIABILITY	6
82H	GEN PUB LAW LIAB (NON-TRIP)	6
82J	ANIMALS	6
82K	DEFECTIVE EQUIPMENT	6
82L	WRKPLACE REGS/SAFETY (PRISONS)	6
82M	CYCLIST	6
82N	ROAD DESIGN	6
82P	FURNITURE/FIXTURES	6
82R	DISEASE (NON-INDUSTRIAL)	6
82S	PEDESTRIAN (NON-TRIP)	6
82T	ADVENTUROUS TRAINING	6
82U	VEHICLE (NON-RTA) ACCIDENT	6
83A	CHALLENGES COSTS OTHER THAN JR	5
83B	COSTS ONLY	5
84A	CLIENT TRAINING	5
84B	CLIENT CARE	5

99	GENERAL	Individual case basis
Lit	Advisory files	5

Appendix 7- File Closure Checklist Label

FILE CLOSURE CHECKLIST

Name (print):

Signed:

Date:

This form must be completed before you send a file to the File Store to be closed and put into storage.

Check whether each of the above statements applies and tick the box if it does.

Appendix 8 - Form for the front of bundle of papers that do not fit into a file jacket (in case files)

BUNDLE OF PAPERS CASE INFORMATION

This form should be completed and placed on the front of every bundle of papers that do not fit into a file jacket in case files.

It should not be used for policy administrative files.

File Reference:	
Disposal Direction	1st Review / destruction date: Month: Year:

Please attach a copy of this form to the front of the bundle of papers and send to the File Store.

The File Store can be contacted on 0207 210 3443 with any queries.

NAME: _____

TEAM: _____

EXT: _____

DATE: _____

Appendix 9 - Guidance Notes on using the Current File Store and Forms to be used

Current File Store (CFS) Guidance

New Current File Store Boxes

Please use the templates below for labelling your CFS Boxes, and ideally type the case reference and case name, or mark clearly in block capitals.

Current File Store _Form C1 - to be attached to lid of box

Current File Store Form C2 - to be attached to short side of box

By placing labels on the short sides of rKIVE boxes instead of on the long sides, we can maximise storage space in the File Store and store three boxes on each shelf rather than two.

It is important that boxes are labelled clearly to avoid any confusion at data inputting stage. Please type or use a marker pen.

When numbering Current File Store Boxes, it is advisable to label them Box 1, Box 2, instead of Box 1 of 3, Box 2 of 3. This will allow further boxes to be added to the sequence if necessary.

The preferred storage method is standard rKIVE boxes, but smaller boxes, map tubes and jiffy bags will also be accepted.

Any overfilled boxes or boxes higher than 25cm will be returned, as there is only 27cm clearance on the shelves.

Collections and Deliveries

To request a CFS box to be collected or delivered to your desk please email currentfilestore@tsol.gsi.gov.uk

(Please avoid emailing individual members of RM staff with Current File Store requests)

The File Store Team will collect/ deliver up to 8 boxes. For larger numbers, please contact Facilities Management to arrange portorage.

The File Store team is not responsible for adding or removing papers from CFS Boxes. If you need to file/remove papers from a CFS box, please request the box back in the usual way.

Alternatively, why not come down to the file store, and a member of staff can show you where your box is stored. (A photocopier is also situated downstairs if required)

Please contact Nick Jackson (File Store Manager) on ext. 3443 or Nick.Jackson@tsol.gsi.gov.uk if you require any further advice.

Form C1 – attach to lid of box

CURRENT FILE- TO FILE STORE

To be completed by Litigation Team Case Officer

File Name and Reference:

Please store this box of papers in the Current File Store

Your name:

Tel extension:

Room Number:

This form must only be completed for the storage of current files and should not be used for requests for archived files

Form C2 – attach to small side of box

Case Ref:
Case Name:
Box No.
Division:

Case Ref:
Case Name:
Box No.
Division:

Case Ref:
Case Name:
Box No.
Division:

Appendix 10 - The Agency's Code of Practice for Data Protection

Office Notice 9/2000

HM PROCURATOR GENERAL AND TREASURY SOLICITOR

THE DATA PROTECTION ACT 1998

Introduction and purpose

1. The guidance set out in this Office Notice underpins the Agency's Code of Practice for Data Protection (Annex A) and has been approved by the Office of the Data Protection Registrar. The Agency is required to comply fully with the Data Protection Act. All staff must follow this guidance and the Code of Practice.
2. Staff have a personal responsibility to comply with the Data Protection Act, and to assist the Agency to comply. The Agency also has a responsibility to tell its staff what they should and should not do under the Act, and that is the purpose of this guidance.
3. Just as staff have the right to expect the Agency to use personal information about themselves in compliance with the Act, so too does everyone about whom we hold personal information.

Some useful definitions

4. In what follows, there are a number of possibly unfamiliar terms which recur, and brief definitions of these are:
 - **data subject** - someone about whom personal data is held;
 - **data controller** - the person or organisation who is responsible for holding personal data;
 - **personal data** - any recorded information about any living individual, set out in such a way that they are, or could be, identified;
 - **processing** - all conceivable manipulations of personal data such as collection, use, storage, disclosure or amendment etc;
 - **relevant filing system** - one that is structured in such a way that information about an individual is readily accessible by reference to the individual or by criteria relating to the individual; and to provide him~ or her with details of personal data held on the subject.

The new Act

5. The Data Protection Act 1988 comes into effect on 1st March 2000. It has the same aim as the previous (1984) Act i.e. to protect the privacy of the individual. It gives individuals certain rights and expectations and will require

those who process personal data to be open about it and to follow sound and proper practices.

6. However, the new Act differs in some significant respects from the 1984 Act. The difference which is likely to have the greatest impact on the Agency is that whereas the 1984 Act applied only to personal data held on computer, the 1998 Act will also apply to personal data held on **paper records** which are in a relevant filing system.
7. There is nothing overly complicated or labour intensive about what the Act requires the Agency and its staff to do, and so long as standard good practice in records management and security are followed, we will meet our responsibilities.

Requirements of the Data Protection Act 1998

8. Under the new Act there are eight Data Protection Principles, which state that personal data must be:
 - processed fairly and lawfully;
 - obtained only for specified and lawful purposes and further processed only in a compatible manner, adequate, relevant and not excessive;
 - accurate and kept up to date;
 - kept no longer than necessary;
 - processed in accordance with the data subject's rights regarding direct marketing, automatic decision making and seriously harmful processing, and perhaps most importantly the right of subject access;
 - kept securely; and
 - not transferred to countries outside the EEA without adequate protection.
9. The first Principle requires that personal data shall not be processed unless at least one of the following conditions is met, and in all cases the processing must be necessary:
 - the data subject has given consent;
 - it is necessary for the performance of a contract with the data subject;
 - there is a legal obligation;
 - to protect the vital interests of the data subject;
 - to carry out public functions;
 - to pursue the legitimate interests of the data controller, unless prejudicial to the interests of the data subject.

Regulatory environment

10. The Data Protection Act 1988 will be overseen by the Data Protection Commissioner (formerly the Data Protection Registrar), who will take action against data controllers (such as the Agency) if they contravene the Act. The Commissioner will also take action against **individuals**, ultimately through the Courts, if it is considered that they, rather than their employer, are responsible for committing an offence under the Act.
11. With few exceptions, data controllers must give the Data Protection Commissioner relevant details. Our Data Protection Officer does this on behalf of the Agency. Our notification includes all our legitimate requirements for carrying out our core business and support functions, such as personnel administration. We have declared from whom personal data will be received; what personal data will be kept; to whom it will be disclosed; and how and why it will be used. Anyone who is keeping records containing personal data which they think might not be covered by the Agency's entry in the register should check with the Head of Records Management.
12. Individuals have certain rights. These are:
 - to make a subject access request;
 - to prevent processing where the processing is likely to cause the data subject substantial and unwarranted damage or distress or where the processing is for the purposes of direct marketing;
 - to object to automatic decision making;
 - to compensation for any breach of the Act.

Subject access requests by staff of the Agency

13. Staff of the Agency who want to make a subject access request in respect of data held about them on the Agency's personnel records should write to the Assistant Director of Human Resources, who will consider the request and provide access to the data as appropriate under the terms of the Act. A reply must be given within 40 days. subject access requests from outside the Agency
14. Any subject access requests received from outside the Agency must be promptly directed to our Data Protection Officer, who will make the necessary enquiries, including consulting the Assistant Director of Human Resources and provide appropriate information to the individual. A reply must be given within 40 days.

Sensitive data

15. The Act introduces categories of sensitive personal data which require that specific conditions are met. Sensitive personal data consists of information as to:
 - the racial or ethnic origin of the data subject;
 - their political opinions;
 - their religious beliefs or other beliefs of a similar nature;
 - whether they are a member of a trade union;
 - their physical or mental health condition;
 - their sexual life;
 - the commission or alleged commission by them of any offence, or any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any Court in such proceedings.

16. The Act requires that at least one of the following conditions must apply for the processing of sensitive data:
 - the data subject has given explicit consent;
 - to comply with the employer's legal duty;
 - to protect the vital interests of the data subject or another person;
 - the information has been made public by the data subject;
 - in legal proceedings;
 - exercising legal rights;
 - to carry out public functions;
 - for medical purposes;
 - for equal opportunities monitoring;
 - as specified by order.

Sensitive data must be processed in accordance with all other principles of the Act and further advice should be obtained from the Head of Records Management before sensitive data is processed.

Exemptions

17. Specific exemptions may apply to disclosure and subject access principles of the Act. These will be considered by the Head of Records Management with appropriate legal advice where necessary. The exemptions most applicable to the Agency are:
 - Legal Professional Privilege - which should only be relied upon if a claim could be maintained in legal proceedings (this exemption applies to subject access provisions only);
 - confidentiality; and
 - third party information.

The effects of the Act on records management in the Agency

18. The Act demands that records are managed properly. Essentially, the Agency needs to know what information we have and where it is, so that it can be located quickly and in its entirety when needed. We need to ensure that Agency record retention policies are followed. Further guidance on Agency records management policies and advice on meeting them is available from the Head of Records Management.

Timetable for implementation

19. As stated above, the 1998 will come into effect on 1 March 2000. On that date the 1984 Act will be repealed in its entirety, and staff must comply with the 1998 Act. There are some transitional provisions, notably one which allows until 24 October 2001 to comply with the new Act for processing of data held on paper which was being carried out as at 24 October 1998. Any new processing (that is processing for a new purpose or the processing of a new type of data or information) started after 24 October 1998 must comply with the 1998 Act immediately. Please contact the Head of Records Management if you are in doubt about whether you have started new processing since then and if you are planning to start new processing.
20. From 1 March 2000 the Agency must comply with those elements of the 1998 Act which appeared in a similar form in the 1984 Act for data held electronically. These are essentially the principles of the new Act excluding the conditions for processing and the rights of individuals to prevent or object to processing. The Agency's Code of Practice for Data Protection must be followed.
21. In essence, although we have until 24 October 2001 before we are required to give individuals access to information held about them in manual records covered by the 1998 Act, we must make information held on computers available to individuals now on request if an exemption does not apply. However, the Home Office has issued instructions that Government should

not wait until the last minute before complying, and must comply immediately where possible to avoid falling foul of the 1998 Act.

22. The guidance set out in this Office Notice replaces existing guidance in the Staff Handbook (10.5). The Staff Handbook will be amended in due course and the guidance updated as necessary as implementation of the Act progresses

Anyone who would like further advice about Data Protection issues should contact Patrick Driscoll, the Head of Records Management (Tel 020 7210 3342 or email Patrick.Driscoll@tsol.gsi.gov.uk).

Annex A

DATA PROTECTION ACT - THE AGENCY'S CODE OF PRACTICE

This Code of Practice must be followed by all Agency staff, and applies to personal data which staff use for their work, whether in the office or elsewhere.

1. Personal data must be processed only if there is a legitimate need and it is necessary for the purposes of carrying out one of the Agency's functions.
2. Staff must comply with the Data Protection Act 1988 at all times.
3. Personal data must be used only for the purpose for which it was collected.
4. Personal data must be checked for accuracy and kept up to date.
5. Team-based, rather than personal, filing systems should be used wherever possible (to make it easier to find specific information).
6. Care must be taken when disclosing personal information to another person or organisation, and it should only be disclosed in circumstances which are compatible with the purpose for which it was collected. If the answer to any of the following questions is 'no' the disclosure should; not be made:
 - do you have the authority to make the disclosure for the purpose for which it is required?
 - do those seeking disclosure have a right to the information?
 - are they who they say they are?
 - have you considered confidentiality, legal professional privilege and the disclosure of third party personal information?
7. The clear desk policy must be enforced as much as your storage equipment allows - lock personal data away, and ensure compliance with the Agency's security policy (for paper and electronic records) set out in the Staff Handbook.
8. Personal data should be kept for no longer than necessary (follow Agency retention policies).

9. Before up a new system, or processing personal data for a new purpose, staff should check with the Head of Records Management that the Agency is registered to do what is intended. Generally, we can only process personal data for the purposes of our business functions, and functions (e.g. personnel) in support of those.
10. Before entering into a data sharing agreement with another organization, staff should speak to the Head of Records Management for advice on special arrangements.
11. Subject access requests, when received from outside the Agency, should be referred to the Head of Records Management promptly.

Appendix 11 - Retention Policy for Private Office records

RETENTION SCHEDULE

PRIVATE OFFICE RECORDS

Record Description	Action by Private Office	Action by Records Mgt
Permanent Secretary's Notebooks	Send to RM at the end of service	Destroy after 5 years
Private secretary's Notebooks	Send to RM at the end of the year	Destroy after 5 years
Permanent Secretary's Official Diaries	Send to RM at the end of the year	Destroy after 5 years
Engagement Diaries	Send to RM at the end of the year	Destroy after 5 years
Declined Invitations (keep on an annual file)	Send to RM at the end of the year	Destroy after 3 years
Registered Files (not invoices or non-TSOL committees)	Send to RM when no longer needed regularly for reference	Review after 3 years
Invoices on Registered Files	Send to RM when no longer needed for reference	Destroy 18 months after end of financial year
Non-TSOL committees on Registered Files	Destroy 6 months after the end of the year	

Destruction or review will be carried out once the period shown in the schedule has lapsed, and will run from the date of last action physically recorded on the file, not from the date it was closed.

This retention schedule has been drawn up by the Head of Records Management in conjunction with the Private Office.

It can only be amended with agreement between the Private Office and the Head of Records Management.