MANAGING NAS RECORDS

a guide for staff

Foreword

We could say that Records ‘R Us. We deal with other peoples’ records every day, from the public registers to historical letters, from government files to court papers. But we also create and use our own records, and that is what this guide is about. Our own records are essential to our work, and we need to manage them carefully. They are a shared asset, of value to the whole of the NAS, not just the branch or unit that created them.

Managing our own records is a fundamental requirement of both the Freedom of Information Scotland Act and the Data Protection Act. Managing our records means having a central records system with practices and procedures for creating, using and disposing of corporate information.

After a lot of study and consultation by our Records Management Unit we have now introduced a new central records system. This manual will help us all to make use of the new system.

Managing our own records effectively will benefit all of us. It will provide us with the information we need to do our jobs, it will avoid us re-doing work that has already been done, it will help us learn from past experience and it will mean we no longer have to search high and low for information.

Please take time to read this manual, and keep it handy for reference. It will make all our work easier.

George MacKenzie
Keeper

April 2003
1.0 Records Management in NAS

Records Management is the systematic control of an organisation’s records, throughout their life cycle, in order to meet operational business needs, statutory and fiscal requirements and community expectations. In NAS that means the management of our corporate information to provide fast, accurate and reliable access to our records, as and when we need them, ensuring the timely destruction of redundant information and the identification and protection of our vital and historically important records.

1.1 What is a record?

The definition of a record is provided in the International Standard on Records Management ISO 15489 it explains records are:

“information created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business”

In the context of NAS this means a record is the information which is produced to support and facilitate NAS’ business activities and which are kept as evidence of that activity. Records may come in many forms, paper, microfilm, digital, documents, maps, or photographs. This manual however deals only with the paper records of the organisation.

1.2 What happens if we don’t manage our records?

If we do not adopt systematic management of our corporate information we could lay our selves open to many problems.

In an unmanaged records environment, on average, up to 10% of staff time is spent looking for information. In terms of wasted time that works out at just under 45 minutes a day. In terms of what this actually costs the office: with an average salary of £18,500, and with a working population of 160 people, that means we spend £292,448 per year on looking for information, over five and half thousand pounds per week!

Then there are the security risks that come with an unmanaged system. If you don’t know what information you have and where it is, then how will you know if someone takes it, loses it or destroys it. New legislation in the form of the Data Protection Act and the Freedom of Information (Scotland) Act, mean that the NAS’ management of its records is now open to more scrutiny. Requests for information governed by statutory response timescales will be very difficult to service if such records are not properly organised and retrievable

An unmanaged records system makes the performance of our duties more difficult, costs the organisation in time, money and resources and makes us vulnerable to security breach, prosecution and embarrassment.
Introduction

1.3 Why is records management important?

The core business of NAS involves the processing of large amounts of information, given the wide range and number of records NAS creates and uses it is essential that they are captured, managed and preserved in an organised system which maintains their integrity and authenticity.

Records contain information that is a valuable resource and an important business asset. A systematic management of records enables NAS to:

• conduct our business in an orderly, efficient and accountable manner
• support and document decision making
• provide continuity in the event of a disaster
• meet legislative and regulatory requirements
• protect the interests of our employees, clients and stakeholders

Sound record keeping practices promote efficiency and economy within NAS. Having comprehensive and timely access to the information contained in NAS records assists everyone in carrying out their duties.
2.0 NAS Records Management Unit.

NAS’ records management unit (RMU) was established to design and administer a records management service in accordance with international best practice and standards. The duties and responsibilities of the records management unit are to:

- oversee and control the opening, closure, issue and disposal of all NAS records, in line with the NAS file classification scheme

- provide a records retrieval service to colleagues throughout NAS’ three buildings

- provide advice and assistance on any records management matters

- prepare, disseminate and maintain records management standards and procedures

- oversee the secure storage of both active and inactive files, to maximise space and cost efficiency

- maintain the file classification scheme

- manage the central review of NAS records, in line with the retention and disposal schedule

- provide training for all staff in NAS records management procedures

2.1 Contacting the Records Management Unit.

The Records Management Unit comprises a central team based in West Register House and a network of local records management officers in every branch.

The central team, which includes a Records Manager and an assistant, are there to provide records management advice. They can be contacted on:

☎ 1437/1415  ✉ recordsmanagement@nas.gov.uk  📍 room 12, WRH

The local records management officers are designated members of each branch who can also provide advice and assistance to staff. An updated list of local officers is available on the Oracle. Local officers retain copies of all NAS Records Management standards and documentation.
3.0 NAS FILE CLASSIFICATION SCHEME

The systematic management of NAS’ records is underpinned by the NAS file classification scheme. The classification scheme is a key management tool which helps users of the NAS records system identify the appropriate file in which to house a particular document, the place of that file in relation to other files and the records management system as a whole, and the life expectancy of that file.

The file classification scheme comes in three parts with an introduction.

3.1 Part A: File plan

The foundation stone of the file classification scheme is the file plan itself. The functions based file plan provides for the systematic framework within which the records themselves will be effectively managed. All records are created as the by products of the activities undertaken in pursuit of the fulfilment of NAS’ functions, each record providing evidence of the activity which generated it. It is logical therefore, that the records of a certain activity be filed together, so as to facilitate better management of that information.

The file plan, which forms the cornerstone of the file classification scheme sets out all the functions and activities which NAS has responsibility for, and arranges them in a logical system. It is this arrangement which sets out the structure of the filing system, predetermining the file series and reference codes.

3.2 Part B: Content guidance

One of the key features of a file classification scheme is the guidance for users of the system as to where in the filing structure a particular document is to be found or housed. The content guidance provides a mapping of all NAS record types, i.e. the types of documents created by NAS, into their appropriate section of the file plan. The aim of the content guidance is to enable users of the NAS filing system to locate and file information.

3.3 Part C: Disposal Schedule

The final feature of the File Classification scheme is the disposal schedule. For the large majority of NAS files the usefulness of the information they contain decreases over time, until eventually it is no longer required. However the rate of deterioration the information depends on the activity from which the record was generated. Records are required to be kept for varying lengths of time for business, legal, regulatory and fiscal reasons, and sometimes they need to be retained permanently. The disposal schedule attaches a disposal instruction to each series of records within the filing scheme, so as to ensure records are kept for as long as they are needed and no more, thus maximising space, resources and efficiency.

3.4 Purpose of the File Classification Scheme

It is within this framework that all NAS records are created, controlled and managed. The scheme is designed to be as flexible as possible, but it is controlled by the records manager so as to ensure filing consistency. It is reviewed annually and changes can be made at any time to reflect changing business activities. To make a change to the file classification theme you should complete an RM5 Addition to the file classification scheme form and send it to RMU.
4.0 Forms and Templates

The records management unit, which oversees the many practices and procedures that make up the records system centrally, controls the records management service. However in practice the records management service operates in a decentralised manner where users have control over the files they create and use.

In order to maintain the system to meet its business needs and user expectations the records management service relies on a number of forms and templates which are used to document file activities, such as the creation of a new file, or the transfer of a file. These forms and templates are referred to throughout this manual where appropriate.

4.1 Where to find forms.

The Oracle has a dedicated Records Management Area where all records management information can be found, including instructions, like this procedures manual, documentation, such as the file classification scheme, and the records management database, which is the central database of all NAS records.

The Records Management area can be found in the Reference section of the Oracle, and in here you will find a link to forms and templates which will take you to the templates of all forms mentioned in this manual. In addition to this you will also find the records management forms templates in the Forms, Documents and Templates section within the Corporate area.

For the most commonly used forms identified in this manual there is a dynamic form facility in the Records Management section of the Oracle. The RM1 and RM2 forms, which are to be used when opening and requesting the use of a file, can be completed on line using the online forms facility. These are automatically submitted to the Records Management Unit by email and this is the recommended method of completing these forms.

Local Records Officer

Your local records officer will also keep a stock of hard copies of all the Records Management forms mentioned in this manual, which can be submitted to RMU via NAS internal mail.

4.2 Submitting forms.

- **Dynamic Forms** All dynamic forms are automatically emailed to the records management unit. The user will receive a receipt when the form is submitted.

- **Via Email** Alternatively you can download a form template, complete this on your desktop and send it to the Records Management Unit at RecordsManagement@nas.gov.uk. Again the user will receive a receipt when the form is submitted.

- **Internal Mail.** You can obviously print off the template and send a hard copy to the records management unit via the internal mail, however this will lead to a slight delay in processing, as it will take longer for the unit to receive the form.
5.0 Creating files

5.1 The Registered File

The registered file is an organised assembly of documents kept together for use, and relating to a specific subject, type of transaction or area of business. If records are not to be lost or misplaced, it is essential that they be registered to a central database which can be controlled by the records management unit.

5.2 Opening a New File

The records management unit, at the request of users, centrally creates all files. To create a new file, or to open an additional part of an existing file, the form RM1 New File must be completed and sent to the records management unit.

In order for RMU to be able to open the correct new file, users must provide the following information:

- Reference
- Title (in full)

and any supporting information.

The reference and the title must come from the file classification scheme in order to be valid.

Deciding which file you need:

1. Before requesting the creation of a new file you should give some consideration as to whether or not you actually need to create the file. Information is an occupational hazard. Producing, filing and storing unnecessary and unimportant information is a waste of space, resources and staff time.

2. In determining the appropriate file theme the user should consult the following:

   file theme index
   The file theme index is a summary overview of all available themes in the file plan, and their corresponding reference. These top-level themes reflect the core functional areas of NAS business, and the activities which make up these core functions.

   subject thesaurus
   The subject thesaurus provides a list of common subject and NAS record types, which are cross-referred to specific themes in the file classification scheme.

   file plan
   The file plan provides a list of all series and file types available for use.

   content guidance
   The content guidance provides a matching of NAS record types to the appropriate section of the file plan.

   All of these documents can be accessed via the Records Management Section on the Oracle, or can be found with your local records management officer.

3. When you have selected the appropriate file theme, remember to check the disposal implications for that particular series. If you think you have selected the correct file theme, but the disposal arrangements are not suitable make a note of this concern in the Additional Information Area of the RM1 form.
Creating Files

4. For each available theme, there are five different types of file available
   I. policy and procedure file
to include information associated with the file theme that relate to policy and procedure
   II. administration file
to include information associated with the file theme that is of a general administrative nature, i.e. records that are created in the course of the operation of our duties that do not affect policy
   III. subject file
to include information associated with the specific theme that relate to a particular subject, event, body, person or product.
   IV. committees file
to include information associated with the specific theme that are generated or received by committees, working parties etc.
   V. reports and statistics file
to include information associated with the specific theme that consist of reports and statistics.

Once you have selected your appropriate theme consider which of these types of files would best suit your needs.

5. You should now have a theme, a file type and a theme reference. You can now complete the new file form and send your request to the Records Management Unit. Only completed RM1 forms will be accepted as requests for a new file.

6. If you are unable to find the appropriate theme in the file classification scheme you should contact your local RM officer for help and advice.

5.3 Opening a new file part

A new file part can be created when a file has to be closed but the business on the file is continuing. The subject of the new file part remains the same.

If a new part of an existing file is required then a completed RM1 form should be sent to RMU, together with the existing file part for closure (the closed part can be reissued to you once it has been formally closed). If the previous part is required for continued use and cannot be returned to the records management unit for closure, the local records officer will be issued with a file closed sheet for that purpose.

In order for the records management unit to be able to open the correct new file part, users must provide the following information:

- Reference
- Title (in full)
and any supporting information.

1. Title: The title for the new file part can be determined from the title of the existing file.

2. Reference: The reference of the file will change. All new files are issued with a part number, when requesting a new file part you should copy the reference from the existing file but change the part number to the next number, for example previous file is part 2, you should request a part 3 be opened.

3. Additional Information: in the additional information section you should note that this is a request for a new file part by completing in block capitals ‘NEW FILE PART’.
Creating Files

5.4 Processing Time

Requests for new files or new file parts received by the submission of a completed RM1 New File form will be issued and sent out to users in accordance with this timetable.

<table>
<thead>
<tr>
<th>Requests received by</th>
<th>Arrive GRH</th>
<th>Arrive TTH</th>
<th>Arrive WRH</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.30</td>
<td>14.30</td>
<td>13.30</td>
<td>13.30</td>
</tr>
<tr>
<td>15.30</td>
<td>10.00 nd</td>
<td>10.30 nd</td>
<td>10.00 nd</td>
</tr>
</tbody>
</table>

All times are subject to the NAS van timetable and mail service, n.d indicates next day delivery. Once a file has been created it will be issued to the user who requested the file creation, in keeping with the procedures for file issue.

5.5 File covers.

NAS file covers are made from rigid manilla board, and are colour coded to ease recognition.

<table>
<thead>
<tr>
<th>NAS1 Private Office Papers</th>
<th>Buff</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAS2 Finance</td>
<td>Blue</td>
</tr>
<tr>
<td>NAS3 Corporate Administration</td>
<td>Red</td>
</tr>
<tr>
<td>NAS4 Record Creators</td>
<td>Violet</td>
</tr>
<tr>
<td>NAS5 Projects</td>
<td>Yellow</td>
</tr>
<tr>
<td>NAS6 Public and Advisory Services</td>
<td>Green</td>
</tr>
</tbody>
</table>

All file covers are pre printed with the major theme, and will have all title and reference information provided by RMU at point of creation.

The file cover has a grid in which to record the file’s circulation when in use. RMU will complete this.
6.0 Searching for a registered file.

As part of the creation process all files will be registered on the NAS Records Management Database. This database is available to all members of staff via its OPAC facility, which can be accessed through the Oracle. The records management database OPAC is a DS Calm application and is very similar to the Archive Catalogue OPAC. Users can use the Records Management OPAC to see what files are on the system and available for use.

6.1 The Records Management OPAC

The records management OPAC is accessed through the Oracle. It can be found in the section Reference/ Records Management/ OPAC.

Upon opening the OPAC you will be faced with a welcome screen which is split into two sections, a main screen and a menu bar. Details about the functions of the records management unit and its contact information can be found on this screen.

To look for a file, you should select the search option on the menu bar which will take you to a search screen with a number of search options:

- **Any Text**: this will search all fields in the database and recover any matches with the word or phrase you have entered.

- **Rec ID**: You can use this option to search using just the file reference, or any part of it.

- **Title**: If you chose this option the browser will search all title fields in the database to find a match with your search term.

- **Description**: If you chose this option the browser will search all description fields in the database to find a match with your search term.
Searching for Files

Once it has conducted the search, the OPAC will provide you with a hit list of records which have matched your search. It will display 20 matching records at a time.

You can navigate through the hit list by using the next and previous options at the top of the screen (identified by the arrow).

Once you have found the file you are looking for, you can get more detailed information about it by clicking on the record number, which can be found to the left of the file reference, and is highlighted in blue. This will take you to a more detailed description of your chosen file, providing a description of the contents of the file and the date of the first paper. Again detailed descriptions can be browsed by using the previous and next navigation buttons.

From the detailed screen you can access an overview of the file’s place in the file plan. By clicking on the file reference you will be taken to the file tree view, which shows all related files.

You can get more information about any file displayed in the tree by clicking on the reference code and highlighted title.

You should use the Records Management Database to find out information about files which have already been created.
7.0 Using Files

Once a file has been created it enters the active use phase of its life, this will be the time when the file will have documents added to it, and when it will be required most for business consultation.

7.1 Requesting a file for use.

If you require the use of a registered file you must complete a RM2 Request for a file form and send it to the records management unit. In order for RMU to find the file users must provide the records management unit with the following information:

- file title
- file reference

This information can be found by conducting a search on the Records Management Database OPAC which is available via the Oracle.

7.2 Processing Time

Once a completed RM2 Request for a File has been received the records management unit will locate the required file. Files which are stored in the record centre will be processed within four hours of receipt of the request, however if a file is already in active use by another member of staff, this may take longer.

<table>
<thead>
<tr>
<th>Requests received by</th>
<th>Arrive GRH</th>
<th>Arrive TTH</th>
<th>Arrive WRH</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.00</td>
<td>14.30</td>
<td>13.30</td>
<td>13.30</td>
</tr>
<tr>
<td>16.00</td>
<td>10.00 nd</td>
<td>10.30 nd</td>
<td>10.00 nd</td>
</tr>
</tbody>
</table>

All delivery times are dependent on NAS Van and mail delivery service, n.d indicates next day delivery.
Using Files

Requests for files in active use

If a file is in active use, the records management unit will contact the user and arrange, if possible, for the file to be transferred to the person requesting the file. However there may be occasions when the file is required by two users simultaneously, in those circumstances flexibility will be required. Delivery times will vary according to the particular circumstances of the file use.

<table>
<thead>
<tr>
<th>Requests received by</th>
<th>From</th>
<th>To</th>
<th>Arrive</th>
</tr>
</thead>
<tbody>
<tr>
<td>1400</td>
<td>WRH</td>
<td>WRH</td>
<td>15.30</td>
</tr>
<tr>
<td></td>
<td>WRH</td>
<td>GRH</td>
<td>09.00 nd</td>
</tr>
<tr>
<td></td>
<td>WRH</td>
<td>TTH</td>
<td>08.30 nd</td>
</tr>
<tr>
<td></td>
<td>GRH</td>
<td>GRH</td>
<td>09.00 nd</td>
</tr>
<tr>
<td></td>
<td>GRH</td>
<td>WRH</td>
<td>11.30 nd</td>
</tr>
<tr>
<td></td>
<td>GRH</td>
<td>TTH</td>
<td>11.00 nd</td>
</tr>
<tr>
<td></td>
<td>TTH</td>
<td>TTH</td>
<td>08.30 nd</td>
</tr>
<tr>
<td></td>
<td>TTH</td>
<td>GRH</td>
<td>11.00 nd</td>
</tr>
<tr>
<td></td>
<td>TTH</td>
<td>WRH</td>
<td>11.30 nd</td>
</tr>
</tbody>
</table>

All delivery times are dependent on NAS Van and mail delivery service, n.d indicates next day delivery

7.3 Issue of files

Once a completed RM2 form has been received and the file located the Records Management Unit will arrange for the issue of that file to the user. All files will be issued with an accompanying loan docket which outlines the conditions of loan:

- all files are issued for a period of sixty calendar days
- all files are issued in the name if the requesting user and they are responsible for its safekeeping
- all files must be stored securely in the designated storage areas, in accordance with NAS security and Access policy
- files must not be passed on to any other member of staff without first completing an RM4 File Transfer form.

Upon receipt of a file users must complete the loan docket and return it to the records management unit.
7.4 Transfer of Files

Occasionally users will be required to transfer files currently issued in their name to another colleague, such transfers can only be initiated by RMU. Files are non transferable unless specifically instructed by RMU.

In these cases the local records officer will be sent a file transfer request, detailing the required file and the user who has requested it. So as to ensure an accurate record of all file movements are kept, the records officer must complete an **RM4 Transfer a File form** and send it to RMU. Once this has been received RMU will action a reissue of the file to the new user, who will then be responsible for the safety of the file.

If files are transferred from user to user without the completion of an RM4 form the records management unit will quickly loose track of the location of files. This will mean that these files may become misplaced over time and staff will no longer be able to access the information on them. In addition, the original file user, who agreed to be responsible for the safekeeping of the file will loose file borrowing privileges for a period of 10 days. It is therefore in both yours and the organisations interests as whole that the procedures for the issue and transfer of files is followed.

7.5 Reissue of files.

If you require to keep the file in active use for a period longer then sixty days you must complete an **RM6 Reissue form**, and return it to the records management team in advance of the end of your loan period.

7.6 Overdue loans.

All files are issued for a period of 60 calendar days, after the sixty days has elapsed files should either be returned to the record centre or reissued.

If files are not returned to the record centre at the end of the loan period a reminder letter will be sent to you on the first day after your loan period has expired. The file must be returned, or a reissue form must be received within 5 working days of the expiry of the loan period or loan privileges will be revoked from that user for a period of 10 working days.

7.7 Return of files.

Files which are no longer required for active business use should be returned to the records centre as soon as possible. They should be sent in a file transfer case, to protect the files, and sent to the Records Management Unit, Room 12 WRH. The local record officer keeps file transfer cases, and supplies can be obtained from the RMU.

When moving protectively marked files around the office a secure transit cases must always be used, secure cases can be obtained from the RMU.
8.0 File Storage

Records are expensive to store and maintain, and if not controlled properly can take up valuable office space. NAS operates two types of record storage.

8.1 NAS Records Centre

The records centre, which is housed in WRH, provides secure, controlled cost efficient storage for NAS’ semi current records, i.e. those which are not required for day to day use in the business area, but are not redundant and may be required for continuing business use on the future.

The records centre has over 200 meters of secure storage for files, and is managed by RMU. Staff can access files in the records centre at any time, by completing the RM2 Request a file form, all requests will be processed within four hours of receipt.

The records centre is equipped with secure storage facilities in which protectively marked semi current records can be stored.

8.2 Active File storage

When files are active and in use day to day, they must be stored in a designated storage facility. Each branch has a limited active file storage facility, which is monitored by the central records management unit.

Each member of staff is allowed up to one metre of active storage space, and each branch has a per capita allocation. Once the allocated active storage space is used up, no more files can be issued to any member of that branch. It is therefore in your best interest to return files as soon as possible, so as to ensure effective storage.\(^1\) Your local records officer who oversees their management will keep a list of designated file storage facilities.

8.3 Storage of Classified Files

NAS records contain information which if disclosed to the wrong people could damage NAS, its staff and its customers. The security and access arrangement, as described in section 13.0, outline the protective markings which are used to control access to NAS corporate information. Whilst files are either in the record centre or in active storage the following arrangements must be followed:

\(^1\) Obviously exceptions can be made to this in cases where additional space is required, but that will not be commonplace.
8.4 File Free Desks Initiative

Many NAS staff work in public areas and many other in shared or open plan offices, in these situations there is a risk that you may accidentally expose confidential material by leaving registered files on your desk, especially when you are away from your desk. When files are made available on unattended desks material could be removed from them and copied or stolen. To ensure that our information is controlled and safe, we would request that colleagues operate a clear desk policy for registered files as far as possible removing them from desks at the end of the working day and returning them to designated secure storage.
9.0 Closing Files

In order to comply with Public Records Legislation, and to remain in keeping with Scottish Executive colleagues, all NAS Files will be closed when they meet one of two closure criteria:

- **5 Years**

No file will remain open for more than 5 years from the date of the first paper on the file. If the file is still live after 5 years, i.e. the subject or activity is ongoing, a continuation part should be opened and the existing file closed.

- **4 cms**

File should not be allowed to become too bulky, 4 centimetres is the maximum width that will allow the protective flap to lie easily over the top paper and a new file should then be opened.

Files can only be closed by RMU. In the case of the time criteria RMU will automatically close files when they reach five years of age. With the latter criteria however users must inform RMU when a file has reached its capacity. The file should be returned to RMU with an **RM3 Close a file** form.

Once a file has been closed it can still be accessed and issued to staff but,

**NO FURTHER PAPERS CAN BE ADDED TO A CLOSED FILE**
10.0 Disposal of Files

Record disposition is the final phase in the life cycle of the registered file, and it ultimately involves two possibilities: destruction or transfer to an archival series. So as to ensure the timely destruction of records of no continuing value, and the effective selection of our vital and important records, all NAS records are subject to review at one or more stages in their life. Review and the resultant disposal actions of destruction or review and preservation of NAS’ administrative records is achieved by two methods working in tandem.

10.1 Automatic Review

A disposal schedule has been developed which provides disposal instructions for all NAS record series as set out in the file classification scheme, and is subject to an annual review. The disposal schedule sets out predetermined disposal arrangements for all series in the classification scheme and they include the following disposal options.

**PRESERVE**  The file series has been selected for permanent preservation in the SRO archive series (c20%)

**DESTROY**  The file series has been identified as having no continued value and will be destroyed upon the fulfilment of a destruction criteria in the form of a number of years; a date in the future or a particular event, e.g.

DESTROY +2  -  Destroy two years after closure

DESTROY 2005  -  Destroy in 2005

DESTROY @IR  -  Destroy at first review.

**CLOSURE REVIEW**  For some record series it is difficult to determine the fate of the file prior to the creation of the contents, which can sometimes be diverse in nature. In these circumstances it is more appropriate that the records manager review the file at the time of file closure.

The disposal schedule has been programmed into the CALM records management database and it will automatically inform the records management unit when a file has reached a particular stage.

10.2 File Review

If it is not possible to determine the fate of a particular file the records manager can conduct and number of reviews of that file throughout its lifetime. As noted in section 10.1 if a file series cannot be given a disposal instruction prior to opening, it can be reviewed upon closure, the first of the three possible reviews a file can be subject to during its lifecycle. At each of the three reviews different disposal potions are available to the records manager.
Disposal of Files

CLOSURE REVIEW When a file is closed it is best practice to take the earliest possible disposal decision to save on time and storage costs.

<table>
<thead>
<tr>
<th>Disposal options at closure review</th>
</tr>
</thead>
<tbody>
<tr>
<td>DESTROY</td>
</tr>
<tr>
<td>DESTROY + ACTION/DATE/YEARS</td>
</tr>
<tr>
<td>PRESERVE</td>
</tr>
<tr>
<td>FIRST REVIEW</td>
</tr>
</tbody>
</table>

FIRST REVIEW Where no decision could be reached either prior to creation or at closure review.

<table>
<thead>
<tr>
<th>Disposal options at first review</th>
</tr>
</thead>
<tbody>
<tr>
<td>DESTROY</td>
</tr>
<tr>
<td>DESTROY + ACTION/DATE/YEARS</td>
</tr>
<tr>
<td>PRESERVE</td>
</tr>
<tr>
<td>SECOND REVIEW</td>
</tr>
</tbody>
</table>

SECOND REVIEW If a decision is not obvious at first review, then the records manager has the option to send the file to second review, which means the file will be reassessed at a date on later than 25 years after opening. Second review is a last resort for those files whose continued use or value is in doubt.2

<table>
<thead>
<tr>
<th>Disposal options at second review</th>
</tr>
</thead>
<tbody>
<tr>
<td>DESTROY</td>
</tr>
<tr>
<td>DESTROY + ACTION/DATE/YEARS</td>
</tr>
<tr>
<td>PRESERVE</td>
</tr>
</tbody>
</table>

2 The review criteria is available as Appendix B to this document.
10.3 Destruction of files.

The destruction of redundant files takes place on a quarterly rotation and is conducted by the records management unit in consultation with staff throughout the office.

By the second month of the quarter Branch Heads will receive a list of files which are due for destruction by the end of that quarter period. Branch Heads will have thirty days to consider all applications for destruction, and can request to view any of the files on the list for further assessment in they so wish. All destruction decisions must be agreed to by the records management unit and the business area before destruction can take place. If the branch head agrees to the destructions (s)he should complete the destruction agreement form which accompanied the list of files and return it to RMU by the last day of the second quarter of the month. A record of all file destruction will be kept for audit purposes.

Preventing Destruction

If the Branch Head disagrees with a destruction decision for a particular file they should complete an RM7 Prevention of Destruction form outlining the reasons why the file should not be destroyed and the recommended alternative disposal action. The Records Manager will consider any such application and will follow up such requests with a decision or meeting within 14 days.

Destruction

All NAS files will be destroyed in line with the arrangements for the destruction of confidential waste.

10.4 Preservation of files

When the disposal arrangements for the file leads to the permanent preservation of the record, the file will be removed from the record centre and sent for archiving.

The records management unit have responsibility for the maintenance of the SRO record series, the archival history of NAS, and selected files will be added to this series.

If a file is required for continuing business use after it has been archives, it can be ordered out, as with any of the archival collections, via the usual order form, which should be completed and given to the appropriate archive attendants. A copy of the SRO catalogue can be found on the Archive OPAC, and in both search rooms.
11.0 Security and Access to Information

NAS records contain information which if disclosed to the wrong people could damage NAS, its staff and its customers. In order to ensure the appropriate levels of security are attached to these records NAS, like the rest of central government, utilises security protective markings which indicate the level of classification of information, and therefore who is allowed access to it.

The security classifications outlined here are in line with those used by the Scottish Executive and the rest of the UK central government. As a small organisation NAS does not process a great deal of classified information, particularly in the upper classifications of TOP SECRET and SECRET, however, these have been included in the available options so as to remain in line with our government partners.

The overwhelming majority of NAS files will not require security classification and will therefore be treated as UNRESTRICTED, unless a classification is identified.

11.1 Security classifications and available descriptors

The protective markings scheme is made up of two types of security restriction, the security classification and the security descriptor. The five security classifications operate in a hierarchy, with the top end of the hierarchy representing the highest level of protection and the other end indicating that there is no restriction on access. The descriptors give an indication of the reasons why a file has been classified.

<table>
<thead>
<tr>
<th>CLASSIFICATION</th>
<th>AVAILABLE DESCRIPTORS</th>
<th>USE IN NAS</th>
</tr>
</thead>
<tbody>
<tr>
<td>TOP SECRET</td>
<td>ALL</td>
<td>Unlikely</td>
</tr>
<tr>
<td>SECRET</td>
<td>ALL</td>
<td>Unlikely</td>
</tr>
<tr>
<td>CONFIDENTIAL</td>
<td>STAFF COMMERCIAL</td>
<td>Regular</td>
</tr>
<tr>
<td>RESTRICTED</td>
<td>APPOINTMENTS MANAGEMENT POLICY MANAGEMENT BOARD PERSONAL</td>
<td>Frequent</td>
</tr>
<tr>
<td>UNRESTRICTED</td>
<td>NONE</td>
<td>Applicable to the majority of NAS records (^3)</td>
</tr>
</tbody>
</table>

---

\(^3\) Additional information concerning the definition of the security classifications can be found in Appendix C.
Security and Access to Information

11.2 Application of security markings

Security classifications and descriptors, where appropriate, can be applied to both files and documents. In a paper environment if one item on the file is given a security classification above unrestricted, then the entire file is given the same marking. The records manager allocates security markings, however they can be upgraded or downgraded by staff.

11.3 Access to classified records

For all files which are classified restricted or above, the disclosure of the information which they contain, even within NAS, will lead to some measure of harm to NAS, therefore access restrictions are associated within each level of classification. The table below identifies which groups of staff have access to information at different levels of classification.

<table>
<thead>
<tr>
<th>CLASSIFICATION</th>
<th>ACCESS</th>
</tr>
</thead>
<tbody>
<tr>
<td>TOP SECRET: ALL</td>
<td>Keeper of the Records of Scotland</td>
</tr>
<tr>
<td>SECRET: ALL</td>
<td>Keeper of the Records of Scotland</td>
</tr>
<tr>
<td></td>
<td>Deputy Keepers</td>
</tr>
<tr>
<td>CONFIDENTIAL: STAFF</td>
<td>Reporting officers</td>
</tr>
<tr>
<td></td>
<td>Countersigning officers particular to the subject of the file</td>
</tr>
<tr>
<td>CONFIDENTIAL: COMMERCIAL</td>
<td>Keeper of the Records of Scotland</td>
</tr>
<tr>
<td></td>
<td>Deputy Keepers</td>
</tr>
<tr>
<td></td>
<td>Branch heads</td>
</tr>
<tr>
<td></td>
<td>Selected staff involved in a procurement project</td>
</tr>
<tr>
<td></td>
<td>Keeper’s Secretariat</td>
</tr>
<tr>
<td>RESTRICTED: APPOINTMENTS/MANAGEMENT/</td>
<td>Keeper of the Records of Scotland</td>
</tr>
<tr>
<td>POLICY</td>
<td>Deputy Keepers</td>
</tr>
<tr>
<td></td>
<td>Branch Heads</td>
</tr>
<tr>
<td></td>
<td>Keeper’s Secretariat</td>
</tr>
<tr>
<td>RESTRICTED: MANAGEMENT BOARD</td>
<td>Keeper of the records of Scotland</td>
</tr>
<tr>
<td></td>
<td>Deputy Keepers</td>
</tr>
<tr>
<td></td>
<td>Finance Officer</td>
</tr>
<tr>
<td></td>
<td>Keeper’s secretariat</td>
</tr>
<tr>
<td>RESTRICTED: PERSONAL</td>
<td>Head of Legal Search Room</td>
</tr>
<tr>
<td></td>
<td>Adoptions Officers</td>
</tr>
<tr>
<td>UNRESTRICTED</td>
<td>All staff</td>
</tr>
</tbody>
</table>
Vital Records

12.0 Vital Records

Vital records are those records without which NAS could not continue to operate. It is the information, which in the event of a disaster is essential to the continued operation of the organisation. Obviously all of the information contained in NAS files is of some importance, for either short or longer periods of time, but only 4% of all NAS records have been classified as vital. These are the records which would contain the information needed to re-establish NAS in the event of a disaster which destroys all other records; these are the records which protect NAS assets and interests and the assets and interests of our clients and customers.

12.1 Vital Records Classification

All series in the NAS file scheme have been analysed to determine which of our records are vital, using a four level classification system.

<table>
<thead>
<tr>
<th>CLASSIFICATION</th>
<th>description</th>
<th>example</th>
</tr>
</thead>
</table>
| Vital          | Records without which NAS could not continue to operate; records which give evidence of legal status, and which protect the assets and interests of the NAS, its clients and customers. | • Minutes of board meetings  
• Accounts receivable  
• Legal documents |
| Important      | Important to the continued operation of the organisation. Can be reproduced from original sources but only at considerable expense | • Procedures manual  
• Collection policy files |
| Useful         | Loss would cause temporary inconvenience to NAS. Replaceable | • Most correspondence |
| Non essential  | No value beyond the immediate purpose for which the records were created | • Readers tickets |

12.2 Vital Record Identification

All files identified as belonging to a vital record series will be identified by a VITAL RECORD label applied by RMU at file registration, this will help to identify files in the event of an emergency.

All vital records are identified in the disposal schedule and the records manager maintains an up to date register of all vital record series. This can be accessed via the Oracle. The register identifies:

- reference
- location of copies
- reasons for protection
- method
- retention
12.3 Vital Record Protection Strategy

So as to protect our vital information a strategy of duplication and dispersal will be adopted. This strategy requires duplicate backups to be made of all vital records at the point of creation. Therefore when a new document is created which is to be added to a vital record series, two copies should be made.

The master copy should be put on the physical file and the duplicate is referenced\(^4\) and sent to RMU by the branch records management representative.

The vital record duplicates accumulated by RMU will be sent to reprographics for microfilming every quarter, after which time the duplicates will be destroyed. Upon completion of the QA process, the vital record microfilms will be labelled and sent to TTH secure storage, whereupon they will be managed in accordance with the retention and disposal schedule.

When new series and documents are created it is the responsibility of the records management representative to liaise with branch colleagues to determine the status of the record although, any recommendation for vital record status has to be approved by the records manager

12.4 Your Vital records responsibilities

**All staff**

- Your local records officer will be informed of all vital files in use in your branch, and will remind colleagues to follow the vital records protection strategy.
- Vital records are identified by the VITAL RECORDS label on the left corner of the file cover.
- when filing to a vital file you MUST make a copy of the document which you are filing
- You MUST reference the duplicate document with the FULL reference of the file in which the master is housed
- You MUST send the duplicate copy to your local records officer immediately who will send it on the RMU forthwith

**Record Officers**

- You must keep your branch informed of any vital files which they use
- You must ensure branch colleagues are aware of the vital records protection procedures.
- You should ensure all duplicates passed to you are fully referenced.
- You should collate all duplicate vital documents from your branch and send them to RMU, identifying them as Vital Records.

\(^4\) The duplicate paper should contain the reference of the file on which the master is housed.
13.0 Filing rules

13.1 General

Files are the case histories which preserve correspondence and are the record of what decisions are reached and what action is taken. Incorrect or slipshod filing makes for mistakes, confusions and unnecessary work. It is therefore essential that files are properly maintained and that the standards procedure for the filing of papers are followed.

**ALL STAFF ARE RESPONSIBLE FOR THE MAINTENANCE OF GOOD FILING PRACTICE.**

15.2 Basic rules:

- In filing papers, the ‘reverse book’ method of filing should be used, i.e. opening the file; the latest paper should be filed on top.
- No matter when they become available papers should be filed in the order of the date on which they were written.
- Files should not start with a paper referring to another paper which is not on that file.
- Attachments or enclosure to documents should be filed immediately below the document to which they relate. Plans, drawings or other bulky items should be put in a pouch with the contents recorded on the front of the pouch.
- Duplicate copies of the same papers should not be filed.
- Newspaper cuttings should not be filed on registered files unless they affect policy.
- When files reach a maximum of 4cms in width they should be returned to the records management unit for closure.
- Files should only be stored in designated storage facilities, they should **never** be stored in personal drawers.
- Guidance on the contents of files can be found in the file classification scheme Part B Content Guidance, which can inversely be used to determine the correct house for a particular document.
- No electronic media should be attached to a registered file; electronic documents of continuing importance should be printed out to file.
- NAS operates a clear desk policy to ensure the security of our corporate information, all files should be returned to secure storage at the end of the working day.
- Sellotape, post-its, paper clips and staples should be removed from document before filing.
APPENDIX A:
NAS Records Management Policy

NAS Records Management Policy

As a result of its functions and activities, The National Archives of Scotland creates and receives administrative records which are a valuable resource and an important asset, as well as supporting our legal, fiscal, businesses and administrative requirements.

The systematic management of NAS’s own records is essential in order to protect and preserve them as evidence of actions, support future activities and business decisions, and ensure accountability to present and future stakeholders and customers.

Recent Government initiatives and forthcoming legislation reinforce the need to be fully accountable and to deliver services in a consistent and equitable manner. They make the setting up of records management procedures important for all organisations and imperative for NAS, as we will be expected to set a good example in this area.

Forthcoming Freedom of Information legislation will include provision for ministers to issue a code of practice on records management. This is likely to require authorities to have in place an overall policy statement on how to manage its records, endorsed by top management and made readily available to staff at all levels of the organisation. In addition, and in line with the UK Government, the Scottish Executive expects all public services which can feasibly be delivered electronically to be online by 2005. In order to meet this target, government departments and agencies must be able to retrieve, appraise and dispose of electronic records efficiently and effectively.

The following policy sets out the procedures and practices needed to control and manage NAS’s own records in such a way that the above requirements are met efficiently and effectively. The adoption of the policy will also bring the following benefits to staff:

- Efficient access to reliable records.
- A clear and understandable filing system.
- Training in those aspects of the system which have a bearing on individuals’ jobs.
- Protection from accusations of unnecessary secrecy under the Data Protection Act and forthcoming Freedom of Information Act.
- A smoother eventual transition into electronic records management, which will allow even faster and more efficient record searching and retrieval.

KEEPR OF THE RECORDS OF SCOTLAND
15 October 2001
# NAS Records Management Policy

## SCOPE OF RECORDS MANAGEMENT POLICY

1. This policy aims to fulfil the requirement for good management of the records which the National Archives of Scotland creates and receives in the course of administering its own business. It does not apply to the records of organisations and private individuals deposited in NAS for historical purposes.

2. The records covered by this policy must meet the legal, operational and archival requirements of the National Archives of Scotland. They must also ensure its accountability to present and future stakeholders and customers.

3. The policy covers:
   - the requirements that must be met for the records themselves to be considered as a proper record of NAS activity
   - the scope of the systems and processes required to ensure the capture, integrity, security, retrievability and correct disposition of NAS records
   - staff responsibilities
   - an implementation strategy across the organisation
   - provision for regular review of the records management policy and its implementation

## RELEVANT LEGISLATION AND REGULATIONS

The policy complies with the following acts, regulations and best practice standards:

- Data Protection Act, 1998
- Human Rights Act, 1998
- Electronic Communications Act, 2000
- International Standard on Records Management, BS ISO 15489
- Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically, PD0008: 1999
- Principles for Good Practice for Information Management, PD0010: 1997

In addition, certain records will be subject to other legislation covering their particular subject area. Branches should ensure that they are aware of the legislation governing their work and its bearing on their record keeping.

## DEFINITION OF A RECORD

A record is information in any medium, created, received and maintained as evidence and information by an organization or person, in pursuance of legal obligations or in the transaction of business.
PRINCIPLES OF GOOD RECORDS MANAGEMENT

The guiding principle of records management is to ensure that information is available when and where it is needed, in an organised and efficient manner, and in a well-maintained environment. In order to do this, NAS must ensure that records are:

Authentic
It must be possible to prove that records are what they purport to be and who created them, by keeping a record of their management through time. The record keeping system will operate so that the records derived from it are credible and authoritative. Where information is later added to an existing document within a record, the added information will be signed and dated. With electronic records, changes and additions will be identifiable through audit trails.

Accurate
Records must accurately reflect the transactions that they document.

Accessible
Records must be readily available when needed.

Complete
Records must be sufficient in content, context and structure to reconstruct the relevant activities and transactions.

Comprehensive
Records must document the complete range of the NAS’s business.

Compliant
Records must comply with any record keeping requirements resulting from legislation, audit rules and other relevant regulations.

Effective
Records must be maintained for specific purposes and the information contained in them must meet those purposes. Records will be identified and linked to the business process to which they are related.

Secure
Records must be securely maintained to prevent unauthorised access, alteration, damage or removal. They must be stored in a secure environment, the degree of security reflecting the sensitivity and importance of the contents. Where records are migrated across changes in technology, NAS must ensure that the evidence preserved remains authentic and accurate.
To achieve the above, the NAS will implement business processes and records management systems which

- Comply with standards and best practices
- Capture evidence of all activities required.
- Manage the content, context and structure of records securely and reliably
- Facilitate re-use of information contained within records
- Enable efficient access to records, irrespective of their location
- Provide a single interface to records relating to any particular business activity, regardless of the records’ media.
- Retain records for as long as they are needed and in the form required
- Retain electronic records on media that permit reliable data migration and/or system modifications
- Protect records from inappropriate access and usage
- Ensure the security of records vital to the NAS’s main functions
- Provide for future system amendments or re-design

This will be done for both paper and electronic records, by:

- Introducing an appropriate registration, classification and indexing scheme for all records. This will include rules on version control.
- Designating secure areas for record storage under the control of trained staff, using a system of one or more registries.
- Developing retention schedules for all NAS records, coupled with annual file reviews by designated members of staff.
- Implementing effective back-up procedures for the maintenance and security of electronic records.
- Implementing a vital records plan to ensure the recovery of records essential for the running of NAS in the event of a disaster, suitable back-up procedures etc.
- Designating to individuals within NAS responsibility for the various activities necessary to maintain such systems
- Providing appropriate training.
STAFF RESPONSIBILITIES

Everyone within NAS is responsible for ensuring that the records they create or maintain comply with the requirements in this policy. Specific duties will be written into job descriptions.

Senior Management

- Senior management recognise the importance of maintaining a corporate memory of events and activities and is committed to providing sufficient staffing, technical and organisational resources to ensure that the above requirements for dealing with records can be achieved and maintained.
- Senior management will make provision for a regular review of the NAS Records Management Policy and will instigate modifications when necessary.

Line Managers

- Familiarise themselves with, and follow, NAS’s records management procedures and practices and ensure that their staff do likewise.
- Ensure that, where necessary, staff have appropriate security clearance to do their jobs effectively.
- Identify staff training needs and arrange for these to be addressed.
- For their own areas, oversee the application of retention schedules and provide input into their development.
- Undertake management and statistical reporting.
- Ensure records are held in appropriately secure conditions, depending on their classification.

Operating staff

- File items promptly and accurately.
- Identify final versions.
- Send information to the relevant people.
- Ensure records can be accessed as needed.
- Protect security-designated information.
- Follow closure and disposition procedures.

Records management system managers and administrators

- Support users.
- Issue guidance and provide training.
- Monitor proper functioning of records management systems.
- Create and maintain security rights
- Ensure records management systems stay in line with developments in best practice.
- Administer the records management and registry systems.
APPENDIX B:
REVIEW CRITERIA

When reviewing a file the records manager will reach a disposal determination based on the following criteria.

**PRESERVE**
The long term storage of files in the archive series is a very expensive option, both in terms of the space the files occupy and the human resources needed to look after them, any unnecessary preservation is costly to NAS and should be avoided. We aim to preserve a maximum of 20% of our administrative records, either through automatic retention or file review. Although long terms storage is a costly option, if a file contains continuing administrative, evidential or continuing historical value then it must be preserved, regardless of cost.

Files will be preserved if their contents meet any of the following criteria:

- **administrative value** - the contents of the file have a continuing business value to the operations of NAS
- **evidential value** - the contents of a file have a continuing legal, administrative or financial use, or they reflect the development of NAS, its structures, policies, or decisions in significant areas of function.
- **informational value** - the contents of the file detail the origins, structure or evolution of NAS
- **uniqueness** - the contents of the file contain unique information which cannot been found elsewhere which adds to the understanding of NAS or its core functions.
- **historical value** - the contents of the file document one of the core activities of NAS, record interesting initiatives; provide greater understanding of NAS; record organisational change, document major activities, document NAS lead role in professional developments. If a record is being preserved for a historical reason not set out above, the reviewer must explain to the records team the reasons for the preservation.

**DESTROY**
Destruction of records is an irreversible act and the records manager will take care to ensure that nothing of permanent historical or administrative value is lost. The vast majority of our records however will lose their value over time, slowly in the first years after closure, and then more rapidly over following years as the information becomes less and less current. This in time will lead to the ultimate destruction of 80% of NAS records. This destruction is an important feature of preservation, and good information management. Files will be destroyed if all the following criteria are met:

- the contents of the file are of no further **administrative** value
- the contents of the file are of no continuing **informational** or **historical** value
- the contents of the file are of no further **evidential** value
- there is no **legal or regulatory requirement** to preserve the contents of the file
## APPENDIX C:
SECURITY AND ACCESS CLASSIFICATIONS

<table>
<thead>
<tr>
<th>CLASSIFICATION</th>
<th>DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>TOP SECRET</td>
<td>Information whose unauthorised disclosure, even within NAS, would be likely to threaten directly the internal stability of the UK or friendly countries; lead directly to the widespread loss of life; cause exceptionally grave damage to the effectiveness or security of UK or allied forces or to the continuing effectiveness of extremely valuable security or intelligence operations; cause exceptionally grave damage to relations with friendly governments or cause severe long term damage to the UK economy.</td>
</tr>
<tr>
<td>SECRET</td>
<td>Information whose unauthorised disclosure, even within NAS, would be likely to raise international tension; damage seriously relations with friendly governments; threaten life directly or seriously prejudice public order or individual security or liberty; cause serious damage to the operational effectiveness or security of the UK or allied forces or to the continuing effectiveness of highly valuable security or intelligence operations; or cause substantial material damage to national finances or economic and commercial interests.</td>
</tr>
<tr>
<td>CONFIDENTIAL</td>
<td>Information whose unauthorised disclosure, even within the NAS, would be likely to materially damage diplomatic relations; prejudice individual security or liberty; cause damage to the operational effectiveness or security of the UK or allied forces or to the effectiveness of valuable security or intelligence operations; work substantially against national finances or economic and commercial interests; substantially to undermine the financial viability of NAS; impede the investigation or facilitate the commission of serious crime; cause serious embarrassment or loss of reputation to NAS;</td>
</tr>
<tr>
<td>RESTRICTED</td>
<td>Information whose unauthorised disclosure, even within the NAS, would be likely to affect diplomatic relations adversely; cause substantial distress to individuals; make it more difficult to maintain the operational effectiveness or security of UK or allied forces; cause financial loss or loss of earnings potential to or facilitate improper gain or advantage to individuals or companies; prejudice the investigation or facilitate the commission of crime; breach proper undertakings to maintain the confidence of information provided by third parties; impede the effective development or operation of Government policies; breach statutory restrictions on disclosure of information; disadvantage Government in commercial or policy negotiations with others; or to undermine the proper management of NAS and its operations. This would normally include records relating to</td>
</tr>
<tr>
<td>UNRESTRICTED</td>
<td>Information whose unauthorised disclosure, particularly outside the NAS, would be inappropriate and inconvenient. This is routine information which NAS simply wishes to keep private.</td>
</tr>
</tbody>
</table>