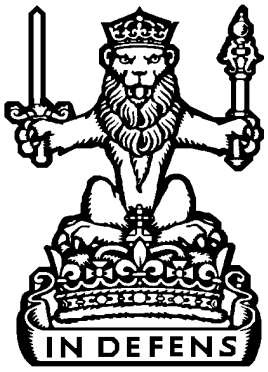

CROWN OFFICE AND PROCURATOR FISCAL SERVICE

RECORDS MANAGEMENT MANUAL

2015

Policy/Common/Records Management/Guidance/ 151026

Approvals and Date for Review

Approval	Date	Further Approval	Date	Actions/Review Due
Records Management Board	April 2010	Area Fiscals Group	June 2010	June 2015
Records Management Board	May 2015	Crown Agent and Chief Executive	June 2015	Updated for NRS October 2015
Records Management Board	October 2015	Crown Agent and Chief Executive	October 2015	June 2016

RECORDS MANAGEMENT MANUAL

CONTENTS

Chapter 1 - INTRODUCTION

1.1 The Public Records (Scotland) Act 2011 (PRSA) places an obligation on named authorities in Scotland to produce a records management plan (RMP) which sets out their arrangements for the effective management of all public records. The Crown Office & Procurator Fiscal Service (COPFS)(named in the Schedule of PRSA as the Lord Advocate and Procurators Fiscal) is an authority defined in the Act.

Policy Statement

Function of COPFS

1.2 COPFS is Scotland's prosecution service. We receive reports about crimes from the police and other reporting agencies and then decide what action to take, including whether to prosecute someone. We also look into deaths that need further explanation and investigate allegations of criminal conduct against police officers.

1.3 COPFS plays a pivotal part in the justice system, working with others to make Scotland safe from crime, disorder and danger. The public interest is at the heart of all we do as independent prosecutors. We take into account the diverse needs of victims, witnesses, communities and the rights of those accused of crime. We support the Strategy for Justice in Scotland and, in particular, its priorities of:

- Reducing crime, particularly violent and serious organised crime
- Tackling hate crime and sectarianism
- Supporting victims and witnesses
- Increasing public confidence and reducing fear of crime

Our values are:

- Being professional
- Showing respect

Our aim is to meet the Law Officers' strategic priority of achieving operational effectiveness in all cases.

The main roles and responsibilities of are to:

- investigate, prosecute and disrupt crime, including seizing the proceeds of crime
- establish the cause of sudden, unexplained or suspicious deaths
- investigate allegations of criminal conduct against police officers.

Our Key Objectives are:

- to secure the confidence of our diverse communities by improving the delivery of justice through the timely, efficient and effective prosecution of crime;
- to give priority to the prosecution of serious crime, including drugs trafficking and persistent offenders;
- to provide services that meet the information needs of victims, witnesses and next-of-kin, in co-operation with other agencies;

- to ensure that all deaths reported to the Procurator Fiscal are investigated appropriately and speedily.

Records Management

1.4 In a records management context, COPFS expects to comply with all legislative and regulatory frameworks which apply to it. The terms of the following legislation are particularly relevant:

- Public Records (Scotland) Act 2011
- Data Protection Act 1998 ,
- Freedom of Information (Scotland) Act 2002 (FOISA) and
- The Environmental Information (Scotland) Regulations 2004

1.5 COPFS recognises that the effective management of its records regardless of format, is essential in order to support its functions to comply with legal statutory and regulatory obligations and demonstrate transparency and accountability.

1.6 Records are a vital information asset and a valuable resource for the COPFS functions and must be managed effectively from the point of their creation until their ultimate disposal.

1.7 It is COPFS policy to maintain authentic, reliable and useable records which are capable of supporting these functions for as long as they are required.

1.8 The COPFS records management plan sets out the policies and procedures for records creation and the policies and procedures in place to manage those records properly.

1.9 COPFS has responsibility for ensuring compliance with this records management policy statement. All staff have a responsibility to manage records effectively throughout their lifecycle, including access, tracking and storage of records; the timely review of records, whether this be for permanent preservation, or confidential destruction or recycling and, where appropriate, their ultimate disposal.

1.10 In addition, COPFS has specific Information Security Policies in place to meet COPFS's essential IT information and network security needs. Many of these policies are pre-requisite essentials for COPFS' accreditation to the PSN and CJX networks. COPFS is required to submit for re-accreditation to these schemes annually (to Cabinet Office for PSN and Home Office for CJX), which involves comprehensive independent IT network health checks, penetration tests and detailed review of technical and policy documentation.

1.11 This Policy Statement and Records Management Manual has been endorsed by the Records Management Board and the Crown Agent and Chief Executive.

1.12 No function of COPFS is carried out by a third party.

Chapter 2 – RECORDS MANAGEMENT ROLES AND RESPONSIBILITIES

Introduction

2.1 The identification of a records management competency framework is a key element of the RMP. The purpose is to outline the knowledge and skills required by the COPFS records manager and other staff who have specific records management responsibilities. By identifying core competencies, the records management staff can manage records effectively, assess training and monitor performance. In addition, all other colleagues are in a position to understand the roles and responsibilities of the records management staff and know who to approach for advice and guidance.

Roles and Responsibilities

2.2 **All COPFS staff** must be aware of the policies, standards and guidance which impact on the way they manage records and information.

2.3 All staff have a responsibility to manage records effectively, through the documentation of all decisions and actions made; the effective maintenance of records throughout their lifecycle, including access, tracking and storage of records; the timely review of records and their ultimate disposal, whether this be transfer to archive for permanent preservation, confidential destruction or recycling.

Named Individuals with Responsibility for RMP

2.4 Catriona Dalrymple, Head of Policy**,** is the senior manager who has overall strategic responsibility for the RMP. This includes responsibility for the implementation of the RMP and for the issue and authorisation of all corporate retention schedules.

2.5 Carol McDivitt, Business Manager, Response & Information Team, is the Records Manager, with overall day-to-day responsibility for the implementation of the RMP.

2.6 The Response & Information Team will have responsibility for:

- issuing corporate guidance for implementing and complying with this policy
- issuing guidance to ensure that staff are made aware of the requirement for the destruction of records to comply with obligations under the Data Protection Act 1998 and Freedom of Information (Scotland) Act 2002.
- developing strategies for the permanent preservation of selected records with the National Records of Scotland
- directing staff to the appropriate information legislation and standards

2.7 **Federation Heads,** together with their **Business Managers**, will ensure:

- that good records management practices as set out in this manual are considered in their business plans.
- that they identify staff (named individuals) within their area to implement the policy so that it is clear who is responsible for making decisions and taking necessary actions.
- that they identify staff (named individuals) within their area to develop local policies for issues which are not covered by the corporate policies.
- that staff have appropriate records management knowledge and skills, through training, where appropriate.
- that the identified staff have this responsibility incorporated into their job descriptions.

2.8 As noted above, each Federation will nominate staff to take local responsibility for Records Management functions, most particularly with regard to the retention and destruction of records. Regular meetings will take place between the Records Manager and nominated staff to ensure that consistent practices are adopted across COPFS.

Records Manager Competency Framework

2.9 The Records Manager has attended a two-day professional course in Records Management practices and has a specific requirement within the job description to attend training workshops and records management conferences at least twice a year ensure that skills and knowledge are kept up to date.

2.10 The Records Manager and other key staff with records management responsibilities require to have training in current COPFS records management best practice and have a specific objective in place in relation to records management responsibility and be able to demonstrate:

- A good understanding of records management issues and best practice and how they relate to the organisation.

- An ability to adapt to and support others in the development and introduction of new recordkeeping practices and procedures.

- An ability to assess current recordkeeping systems and provide feedback to the records manager on their strengths and areas for improvement.

- An ability to communicate effectively at all levels of the organisation.

- An ability to recognise potential issues in relation to records management and communicate these to the relevant staff.

- Enthusiasm and a proactive approach to improving recordkeeping practices.
- A good understanding of the legislative environment within which they operate.
- An ability to contribute to the development and implementation of new records management systems and solutions.
- An understanding of how good records management can lead to improved business efficiency and working practices, as well as other organisational benefits.
- Flexible and adaptable to change.
- An ability to apply records management principles and practices to own work role and work of others.
- An ability to monitor and feedback compliance with policies/procedures.
- An understanding of different types of risk, in relation to recordkeeping.
- An ability to work under pressure and to deadlines.
- Accuracy and attention to detail.
- Problem-solving skills.
- An awareness of information, advice and guidance sources within COPFS.

Chapter 3 – GENERAL PRINCIPLES OF GOOD RECORDS MANAGEMENT

Creating and capturing records

3.1 To carry out its business functions, COPFS must rely on records. Records need to be created to provide a full and accurate source of evidence and information about what we do as an organisation, both for our own staff and external stakeholders. Records can include paper, electronic, e-mail and multi-media documents.

3.2 In order to comply with statutory and regulatory requirements, such as the Public Records (Scotland) Act 2011, the Data Protection Act 1998 and the Freedom of Information (Scotland) Act 2002, it is essential that records are captured into shared recordkeeping systems so that they can be located when required.

3.3 COPFS must identify the records which need to be created and received to document business activities and ensure that they are complete, accurate and up to date.

3.4 While ownership for the creation of records will rest with Federation Heads and their Business Managers, all staff will have varying degrees of responsibility for creating and maintaining records.

3.5 Records should be arranged in a logical filing system, so that files and documents can be quickly located and retrieved and easily identified when the time comes for review or destruction.

3.6 Adequate shared record keeping systems must be developed to ensure that documents are not stored in personal files or mailboxes, but can be located and retrieved when required.

3.7 In a records management context, an effective recordkeeping system is any means of arranging records in such a way as to reflect their business context so that retention can be easily and securely managed in a consistent manner and so that records can be easily retrieved.

3.8 Electronic records must be reviewed, archived and deleted in the same way as paper records.

3.9 Retaining records in personal systems, such as inboxes, must be avoided. Such records are inaccessible to other users and as such are not easily retrievable as part of the corporate record. They are also less likely to be retained for the appropriate retention periods. Therefore, where a hard copy file exists, copies of e-mails, word documents etc which require to be kept for business purposes, should be printed out and kept. Where the

retained file is electronic, e-mails and other associated documents must be kept in a shared folder which can be accessed by all members of the team.

3.10 Documents which are subject to amendment as they are developed should be properly identified by version control to ensure that the latest version or master copy is easily identifiable and managed appropriately.

3.11 Unnecessary duplicate copies of records should not be created.

3.12 Sufficient information (metadata), that is, information which describes what the record is about, must be captured and associated with records to help interpret, retrieve and manage them. Typical metadata would include, but is not restricted to, author, date, file reference and title.

Storing and maintaining records

3.13 Records should be stored in appropriate systems, locations, conditions and in equipment that is appropriate to their media, format and security.

3.14 Electronic information requires to remain accessible, readable, usable and capable of being relied upon for as long as it is required.

3.15 Access rights require to be controlled to ensure that records and record keeping systems are secure where issues of sensitivity and importance exist.

3.16 Business continuity plans must include reference to the protection and recovery of records.

3.17 Where possible, paper records should be retained in storage facilities in office premises. Where this is not possible, it is the responsibility of the local business managers, in conjunction with Estates Division, to acquire premises which meet the above criteria.

Retaining and disposing of records

3.18 It is essential for COPFS to have retention policies to review how long records need to be kept to meet legal obligations and business needs. The retention of unnecessary paper and electronic records takes up staff time, space and equipment. It also incurs liabilities in terms of the need to service requests for information under the Data Protection Act 1998 (DPA) and the Freedom of Information (Scotland) Act 2002 (FOISA). In addition, the DPA requires us to keep records for no longer than necessary and we can be sued for retaining unnecessary information if this causes damage to someone.

3.19 Records should be disposed of in line with their retention schedule. However, staff must bear in mind that in certain circumstances it may be a criminal offence to inappropriately destroy records. You should not destroy

records which are subject to a current request for information until 40 days after the request has been answered. If you need to check whether a record is subject to a Freedom of Information request, or subject access request, please contact the Response and Information Unit.

3.20 All copies of records must be securely disposed of, with consideration given to the sensitivity and security classification.

3.21 Chapter 6 of this Manual sets out the retention periods for case-related records. Hard copy paper records will be reviewed in Dumbarton Disposals and local offices for destruction at the appropriate times.

3.22 The Electronic Data Retention Policy compliments the paper policy. A record will be kept of electronic case records which have been identified for destruction through the electronic data retention policy. This will be managed through ISD.

3.23 Retention Schedules for non-case related information are attached at Annex 4. Responsibility for authorising the disposal of these records must to be assigned to named individuals.

.

Chapter 4 – STORAGE FACILITIES

4.1 COPFS has a storage facility for closed case papers in Dumbarton. It houses the West Federation papers, for the appropriate retention periods as set out in Chapter 6 of this manual. It also holds other categories of record from elsewhere in Scotland as specified below.

Summary Cases

4.2 Summary cases are now fully electronic. Any associated hard copy papers should be scanned into the Case Directory and papers destroyed thereafter in local offices. Summary case scanning is not carried out in Dumbarton.

Sheriff and Jury Cases

4.3 West Federation Sheriff and Jury Case papers should not be sent to the Disposals Unit until the Appeal period of 21 days has passed and PRN has been completed. Case Papers must be in the following order:

- Minute sheet(s) placed at front of case.
- Correspondence file place at back of case.
- Copy signed PRN if relevant placed in correspondence file
- Papers kept in folder.
- Date of disposal and cull date (2, 5 10 years etc) written on front of folder
- Papers sorted in date of disposal order.
- All productions must be removed (Medical Records etc)

Please note that Dumbarton cannot accept papers which have not been reviewed and reduced. Any papers which have not been properly reviewed will be returned to the office concerned.

North and East Federation offices should manage the records locally in the same way.

Deaths and FAIs

4.4 West Federation deaths and FAI papers are retained in Dumbarton for the retention period set out in Chapter 6. Before an FAI case leaves the office for Dumbarton, consideration must be given to whether it is likely to be of long term interest and suitable for permanent preservation at the National Records of Scotland (NRS) – see FAI section in Chapter 6. Cases for permanent retention should be marked "FAI for permanent retention at NRS – transmit in (insert year, which should be 5 years after date of closure)". If a decision cannot be made at that time, the papers should be clearly marked

for review in 5 years' time by the local office. It is not anticipated that many cases will fall into the permanent retention category.

4.5 North and East Federations should send FAI records for permanent retention to Dumbarton at the 5 year mark for onward transmission to NRS.

High Court Papers

4.6 West Federation High Court papers which have not yet been closed for 10 years are retained in Dumbarton.

4.7 Crown Office High Court papers, which are between 2 and 10 years old are also retained in Dumbarton. The most recent two years (current year + 1) are retained on Crown Office premises.

4.8 It has been the practice for Crown Office high court papers to be retained permanently at NRS and files are transmitted once they are 10 years old. Papers which are subject to appeal will be retained on COPFS premises for a longer period, determined by the appeal process. However, it has been recognised that there is valuable information on the PF high court file which is not duplicated on the Crown Office file. Therefore, the following information from the PF high court file must be retained:

1. Minute sheets
2. Petition
3. Custody Statements
4. SPR
5. Correspondence file
6. Disclosure File
7. Any other relevant material which is not contained within the Crown Office papers. The Precognition Officer/Depute who was involved in the case preparation should advise if any other documents are worthy of retention.

4.9 An exercise has now been carried out in Dumbarton to review old high court PF papers up to 2001 and these papers from the West Federation have now been transferred to NRS. However, offices will require to review and reduce their papers on an annual basis prior to the annual transmission in December. Offices must contact the Disposals Unit in Dumbarton to arrange to review these papers in good time. This practice will only be required until the 2011 papers are due for transfer. This is because since 2011 the practice has been to amalgamate PF papers with the Crown Office set immediately after the case is closed. The current year + 1 year are retained in the basement of Crown Office.

4.10 NRS require the case papers to be sent in a folder (obtainable from Disposals Unit) and accompanied by an index.

Other Crown Office records in Dumbarton

4.11 In addition, the Dumbarton facility also holds the following Crown Office records:

- **Civil Recovery Unit files** – marked with the date of destruction
- **International Co-Operation Unit files** – marked with the date of destruction
- **Serious Organised Crime Division files** – marked with the date of destruction

Access to case papers from Dumbarton

4.12 If you require access to case papers that cannot be viewed/printed from the case directory in SOS-R you should complete a Retrieval of Papers request detailing the documents you require and e-mail it to the Disposal Unit Mailbox (Disposals)

4.13 The required documents will be scanned into the case directory in SOS-R where they can be accessed on line. It should only be in exceptional circumstances (or where an appeal is lodged out of time or referred back out of time by the SCCRC) that hard copy papers are returned to the office.

4.14 Where hard copy papers are required, they will be sent by tracked DX Mail or delivered by Disposals Unit staff.

4.15 Non-case papers will also generally be scanned back and only in exceptional circumstances will they be returned hard copy.

North and East Federations

4.16 North and East Federations have separate arrangements for the retention of papers. An exercise is currently being carried out to mirror the processes in the West Federation. It is essential that the premises used for storage of records are secure and free from the possibility of fire and flood. Records must be reviewed on a regular basis and only retained for the period required for business need. Case records are subject to the retention periods set out in Chapter 6.

4.17 Finance Division and Human Resources records are subject to records retention periods which are set out in the Records Retention Schedules at Annex 4.

Chapter 5 - MANAGEMENT OF CASE-RELATED RECORDS

Electronic records and Case Management System

5.1 Case-related information is held within electronic systems which are developed and maintained by the Information Systems Division(ISD). Further details about the functions of ISD can be found on PF Eye.

5.2 The Future Office System (FOS) is the current software, providing COPFS with an easier way of displaying and changing information we store in our database i.e. accused (subject), witness, charge information etc. It also allows us to produce case documents in an electronic format and introduces the concept of on-line case marking.

5.3 The following systems are also currently in place and a summary of their functions is attached at Annex 2.

- PROMIS
- POLIN – Electronic Documents
- COPLINK
- SOS-R
- CHS link
- SLAB link

5.4 Detailed operational guidance and task instructions on the processing of criminal reports and death reports are contained in the Case Processing Manual.5 Case-related information is received electronically and processed this way. The electronic Data Retention Policy has been prepared to compliment the retention periods set out in Chapter 6 of this manual which was primarily developed for paper records.

5.6 Summary case records are now produced electronically. No paper record is kept and the cases are subject to the retention period set out in Chapter 6. Solemn cases are retained as a mixture of paper and electronic records. The paper and electronic records are retained for the identical time periods as set out in Chapter 6. High Court records are not included in the electronic Data Retention policy.

5.7 Case-related information which is not generated in the electronic record (eg emails between members of staff), must be added to the case record so that the full records is maintained. In High Court cases, it is permissible to print off the email chain and to retain it with the hard copy papers

Only the final version of an e-mail trail need be kept, but it is important to ensure that all of the essential comments are included in the thread. If more than one thread exists, all decisions must be included.

5.8 The following provides examples, though not an exhaustive list, of the types of e-mail which require to be printed off and kept hard copy:

- Where a decision is taken in relation to a prosecution
- Where it directly relates to an accused or the case
- Information or opinion which has a bearing on the decision to be taken (eg situation with regard to X, leading to a decision on Y)
- Direct relevance or impact on case – eg problems with witnesses/attendance etc
- Contact with criminal justice partners
- E-mails instructing forensic examination
- E-mails between reporting officer and precognoscer

5.9 If the case is in FOS or SOS-R, e-mails can be imported directly into the electronic record.

5.10 E-mails associated with the case must be kept in the official case record and not in personal mailboxes so that all material is kept together. This will ensure that any member of staff who has cause to access the case will be in a position to read all the relevant information. This ensures that the most up to date information is available and that it can be held for the appropriate retention periods. It also means that we can be confident that all material held can be easily considered should a freedom of information or data protection request be received.

5.11 Business Managers have responsibility at local level for preparing desk instructions for the making up of case files and for arranging appropriate storage facilities. Guidance on what requires to be kept when weeding files, together with the order in which it needs to be kept is provided at Annex 1.

Secure Disclosure Website

5.12 COPFS holds a copy of documents which have been disclosed to the defence. These are basically case documents from FOS/SOS-R, such as witness statements from Police Scotland. We also hold the case information, such a witness name, subject name, production name etc.

5.13 The Secure Disclosure Website allows COPFS to process disclosure electronically to defence agents. Defence agents require to sign up to participate, install required software which is supplied by COPFS by way of pendrive. Defence agents require a user name which is their Legal Representative ID and a password to access each download on the website. When disclosure is sent to the website by COPFS, an email alert is automatically created and sent to the defence agent. This email gives the defence agent, the subject name and a binder id along with a link to the website. On selecting the email link, the defence agent will be prompted for their user name and password.

Respond

5.13 In addition to the electronic case management system we also use the Respond system to log and process customer feedback (that is complaints, compliments, comments and suggestions which are received by the Service, Ministerial Correspondence and request for information (freedom of information requests, environmental information requests (EIRs), subject access requests, and requests for sharing of data from other organisations (falling under chapter 17 of the Book of Regulations)

5.14 While these systems are sometimes used to record requests for information which are not case-related, staff must bear in mind that the systems may also include additional information and correspondence which is directly relevant to a case and which is not held on the case management systems.

5.15 All members of staff can log such requests on to the Touchpoint Respond system via the home page of PF Eye. (See Hot Topics – Quick Links – Respond) and view the progress of these requests.

5.16 However, once the request has been logged, it must be passed on to the Response and Information Unit for attention. Local Respond Co-ordinators around the country also have licences to add, update and ultimately close the record.

Ministerial Correspondence System

5.17 The Ministerial Correspondence System is administered by the Law Officers' Private Office in Crown Office.

5.18 This system is used for logging correspondence from MSPs, MPs and correspondence from members of the public which is specifically addressed to the Law Officers.

Checking Respond and Ministerial Correspondence System for relevant case-related information

5.19 It is particularly important to check all systems to ensure that all information is to hand when answering Freedom of Information and Data Protection requests. You should, as a matter of routine, make a search of the Respond system and check with the Private Office to ensure that all material is considered before answering the request.

5.20 It is also good practice to cross-refer case numbers, on the Respond and Ministerial Correspondence systems and make a note of the corresponding Respond/Ministerial Correspondence reference number on FOS.

5.21 Where it is appropriate, particularly in relation to a live case, the Response and Information Unit will place copies of responses to complaints in the case directory record.

Retention Periods for Respond

5.22 It is intended that information recorded on Respond and any related hard copy files will be kept for 5 years after the last item on file and then destroyed. This is currently work in progress.

Chapter 6 - RETENTION PERIODS FOR CASE RELATED RECORDS (paper)

6.1 This guidance supersedes Crown Office circular 29/2001.

High Court Case Papers and Section 76 Case papers

6.2 At the conclusion of trial, where no appeal is lodged, one comprehensive file will be retained in Dumbarton.

6.3 All papers of evidential value must be retained. This will include:-

1. Precognition backing sheet which includes minutes
2. Precognition
3. Minute sheets
4. AD notes
5. Section 76 Indictment (if applicable
6. Indictment (original and amended version(s))
7. Section 67 notices
8. Copy of execution 67 notice
9. Petition
10. Custody statements
11. SPR
12. Witness statements (original)
13. Witness statements (redacted/disclosure)
14. Disclosure File
15. Crown Counsel's instruction
16. Section 76 report (if applicable)
17. Minutes of agreement
18. Bail Appeal report (if applicable)
19. Transcripts of Judicial Examination (applicable)
20. Transcripts of Police interview tape (applicable)
21. Copy Documentary productions
22. Copy of any photographs
23. Copy of any medical records
23. Correspondence file (with most recent correspondence on top)

6.4 The majority of these papers will exist within the Crown Office file, but within one month of the conclusion of the trial, PF offices must send their papers to Dumbarton Disposals where they will be reviewed to include the following papers with the file:-

- Minute sheets
- Petition
- Custody Statements
- SPR
- Correspondence file

- Disclosure File
- Any other relevant material which is not contained within the Crown Office papers. The Precognition Officer/Depute who was involved in the case preparation should advise if any other documents should be forwarded to complete the record.

6.5 Any videos/tapes should be removed from the case file before it is transferred to Dumbarton and returned to the originator.

6.6 Papers should be removed from any hard folders (which make storage bulky) but tagged together so that they do not become separated.

6.7 The papers should be clearly marked with the case reference number, the court where the case was heard and the date of trial.

6.8 There will be occasion when further correspondence is received in relation to a closed case. In these circumstances, the PF Office concerned and the High Court Unit in Crown Office should discuss who is best placed to provide a response. This will depend on the nature of the correspondence. Where it is agreed that the PF office should reply, all papers will be returned to the office for that purpose. Once the reply has been sent, the papers should be returned again to Dumbarton without delay.

Appeals

6.9 If an appeal is lodged, the papers should be retained in PF Offices until conclusion of the appeal. At this stage the papers which only existed in the PF set of papers should be transferred to Crown Office for amalgamation with the Crown Office papers. This would include:-

1. Minute sheets
2. Petition
3. Custody Statements
4. SPR
5. Correspondence file
6. Disclosure File
7. Any other relevant material which is not contained within the Crown Office papers. The Precognition Officer/Depute who was involved in the case preparation should advise if any other documents should be forwarded to complete the record.

6.10 In circumstances where a late appeal is lodged, and new defence agents have been appointed, papers will be returned to the local office for the appropriate action to be carried out.

National Records of Scotland

6.11 The papers in each High Court case will be retained on the premises at COPFS for a period of 10 years after the conclusion of trial or appeal proceedings and then transmitted to the National Records of Scotland (NRS) for permanent preservation. This also applies to Serious and Organised Crime Division papers which are currently stored separately. Productions in SOCD cases are not to be sent to NRS and can be destroyed at this stage.

6.12 The transmission of high court cases takes place in December of each year and an index is produced by Dumbarton Disposals of all the transmitted cases. This list commenced in 2007, with papers transmitted from 1996. A copy of this list is available to view on PF Eye under Home Page - Guidance & Resources – High Court. The list will be added to each year and the new list will be available the following January.

Older papers retained in PF offices

6.13 All High Court Cases prior to those closed from the beginning of 2011 must be retained by Procurators Fiscal (or Dumbarton Disposals for West of Scotland) for a period of 10 years after the conclusion of trial or appeal, whichever is later. PF offices/Dumbarton Disposals should then:

- weed the papers, removing all duplicates, and retain

    1.Minute sheets
    2.Petition
    3.Custody Statements
    4.SPR
    5.Correspondence file
    6.Disclosure File
    7.Any other relevant material which is not contained within the Crown Office papers. The Precognition Officer/Depute who was involved in the case preparation should advise if any other documents should be forwarded to complete the record.

- Remove papers from binders and place them in soft covered files, with no elastic bands or paper clips
- Where necessary, arrange for transfer of these papers to Dumbarton Disposals by end of November so that the papers can be included in the annual transmission of papers to NRS.

6.14 If an appeal is lodged, the papers should be retained for 10 years after conclusion of the appeal before review. The above procedures should then be adopted.

Sheriff and Jury

6.15 The following categories must be retained for 10 years prior to destruction:-

- Sexual Offences
- Cases where the Procurator Fiscal considers retention is necessary for the purposes of risk assessment

6.16 Otherwise, all Sheriff and Jury papers must be retained for a period of five years after the conclusion of the trial or appeal proceedings or for the length of the sentence if the case has been the subject of a remit.

6.17 There will be a residual discretion for Procurators Fiscal to identify and retain cases of significant legal or historical interest. Such cases should be retained for a maximum of 10 years. If at the conclusion of that time, it can be justified that the case is worthy of permanent preservation, it should then transferred to Dumbarton Disposals for onward transmission to NRS.

6.18 The following is guidance on what requires to be kept when weeding Sheriff & Jury papers and in what order:

1. Precognition backing sheet which includes minutes
2. Precognition
3. Minute sheets
4. Section 76 Indictment (if applicable
5. Indictment (if more than one version then one of each)
6. Section 67 notices
7. Copy of execution 67 notice
8. Petition
9. Custody statements
10. SPR
11. Witness statements (original)
12. Witness statements (redacted/disclosure)
13. Crown Counsel's instruction
14. Section 76 report (if applicable)
15. Minutes of agreement
16. Bail Appeal report (if applicable)
17. Transcripts of Judicial Examination (if applicable)
18. Transcripts of Police interview tape (if applicable)
19. Copy Documentary productions
20. Copy of any photographs
21. Copy of any medical records
22. Correspondence file (most recent correspondence on top)

Summary Cases

6.19 Summary case records are now retained electronically. Hard copy records are scanned and kept with the case record for the following retention periods. Papers are then shredded. ISD will arrange for destruction at the appropriate stage. The records will be retained for the period set out in the Electronic Data Retention Policy.

6.20 There is a discretion for the Procurator Fiscal to identify any papers which should be retained for a longer period of time. However, closed cases should not be retained in a PF office for longer than 10 years. Any cases which can be justified as being worthy of permanent preservation should be transferred to Dumbarton for onward transmission to NRS.

6.21 The following are the records which will be retained for the appropriate retention period:

1. Court minutes
2. Copy complaint
3. Custody statements (applicable)
4. SPR
5. Witness statements (original)
6. Witness statements (redacted)
7. Minute of Agreements
8. Bail appeal report (if applicable)
9. Correspondence file (most recent correspondence on top)

Complaints against the Police (CAP)

6.22 For cases where the officer is prosecuted on indictment, associated CAP papers should be retained for 10 years.

6.23 For cases where the officer is prosecuted by summary proceedings, the associated CAP papers should be retained for 2 years.

6.24 For cases marked no proceedings, the associated CAP papers should be retained for 2 years. However, where the charges relate to a sexual offence, the papers should be retained for 10 years.

6.25 For cases where there is a CAP investigation and an associated prosecution of the complainer in the CAP, but no prosecution of the police officer, the CAP papers should be retained for the same period as the associated criminal prosecution.

6.26 The following is guidance on what requires to be kept when weeding complaints against the police papers and in what order:

Complaints Against Police Cases (No Proceedings):-

1. Police report
2. Witness statements (original)
3. Correspondence file (most recent correspondence on top)

Complaints Against Police Cases (Summary Proceedings):-

1. Court minutes
2. Copy complaint
3. Police report
4. Witness statements (original)
5. Witness statements (redacted)
6. Minute of Agreements
7. Correspondence file (most recent correspondence on top)

Complaints Against Police Cases (Solemn Proceedings):-

1. Precognition backing sheet which includes minutes
2. Precognition
3. Minute sheets
4. Section 76 Indictment (if applicable
5. Indictment (if more than one version then one of each)
6. Section 67 notices
7. Copy of execution 67 notice
8. Petition
9. Police report
10. Witness statements (original)
11. Witness statements (redacted/disclosure)
12. Crown Counsel's instruction
13. Section 76 report (if applicable)
14. Minutes of agreement
15. Transcripts of Judicial Examination (applicable)
16. Transcripts of Police interview tape (applicable)
17. Copy Documentary productions
18. Copy of any photographs
19. Copy of any medical records
20. Correspondence file (most recent correspondence on top)

No Proceedings and Alternatives to Prosecution
Fixed Penalties and Conditional Offers of Fixed Penalties under the Road Traffic Acts

6.27 These cases are now recorded on FOS and no paper copies are kept. Any associated correspondence which is received hard copy, however, should

be scanned into the case directory. Records are retained for the period set out in the Electronic Data Retention Policy set out at 6.70 below.

No pro meantime

6.28 These are "live" cases and do not fall within the retention policy and should be retained in local offices Current guidance is contained in the Case Marking Guidance.

Cases involving Disqualification from Driving

6.29 Papers are to be retained for two years or for the period of disqualification, whichever is longer.

Probation Orders CSOs etc

6.30 Papers are to be retained for one year after the end of the probation period.

Fatal Accident Inquiries

6.31 All Fatal Accident Inquiry papers should be weeded at the conclusion of the Inquiry to remove all duplicate paperwork and retained for 5 years. West Federation offices which use Dumbarton for storage may send their papers there immediately for retention. However, consideration should be given at this stage whether the case is suitable for permanent retention at the NRS. This will apply to cases where there has been a high level of public or press interest, or where there is a continuing interest. It is not anticipated that many cases will fall into this category. It may not be known at the conclusion of the FAI that there will be a continuing interest and in those circumstances it will be the responsibility of the local office to advise Dumbarton of the need to retain the record permanently.

6.32 For all other offices, FAI records will be retained subject to local arrangements, but after 5 years, those which are deemed to be suitable for permanent retention should be sent to Dumbarton Disposals in November of each year so that they can be included in the annual transmission to the NRS. The papers should be clearly marked "FAI – For transmission to NRS + (Details of Case)". This office should retain an index of all cases which have been transferred in this way.

6.33 Ring binders/lever arch folders and elastic bands are not suitable for long term preservation and papers should not be forwarded in such folders. You should exchange any such folders for paper files and use treasury tags to keep the papers together.

Deaths

6.34 Deaths papers should in general be retained for five years.

6.35 This does not include

- deaths which have been the subject of a Fatal Accident Inquiry, which will be kept for 5 years after the conclusion of the FAI
- deaths where there has been a criminal investigation, which will be kept for the appropriate retention periods relating to level of case and
- deaths which have been marked no pro meantime.

6.36 From a disclosure perspective, deaths papers need to be kept for at least the same length of time as any associated prosecution papers.

6.37 The following is guidance on what requires to be kept when weeding deaths papers and in what order:

Routine Death Cases:-

1. Minute backing sheet
2. F5 Notification of Death
3. Police/Death report
4. Notification to Registrar
5. Correspondence File (most recent correspondence on top)

Investigated Death Cases:-

1. Minute backing sheet
2. F5 Notification of Death
3. Police/Death report
4. Post Mortem report
5. Toxicology report (if applicable)
6. Histology report (if applicable)
7. Witness statements (original)
8. Witness statements (redacted/disclosed) (if applicable)
9. Precognition (if applicable)
10. F11 Petition for FAI (if applicable)
11. Books of photographs
12. Copy of documentary productions
13. Correspondence file (most recent correspondence on top)

Victim Information & Advice (VIA) Papers

6.38 VIA letters and other correspondence should be integrated with the electronic case record and not kept separately. They are subject to the same retention period as the case record.

Tapes and Photographs

6.39 Audio/Video/DVD recordings and photographs should be retained for the same period as case papers unless marked for destruction by a Depute at an earlier stage.

Occurrence Reports

6.40 While the police no longer submit Occurrence Reports to COPFS, those which are in existence should be kept for the same period as the nature of the occurrence (eg if it relates to a sexual offence, then the retention period would be 10 years).

Production Books

6.41 Productions books must be retained for 10 years before destruction.

SERIOUS AND ORGANISED CRIME DIVISION

6.42 Where SOCD have ownership of a High Court case, all the High Court papers should be retained for a period of 10 years at Crown Office or Dumbarton storage facility prior to being transferred to the NRS. Papers should be weeded out before being sent to the NRS, with only relevant court papers being retained. Copy productions will not be kept for permanent preservation.

6.43 If there is also a restraint and confiscation case relating to High Court papers when this is closed the restraint/confiscation papers should be stored with the High Court papers after being weeded out.

Sheriff and Jury Cases

6.44 All Sheriff and Jury papers should be retained for a minimum of five years after the date of right of appeal has lapsed.

6.45 Papers should then be destroyed or sent to NRS to be retained for historical interest.

Money Laundering

6.46 If a criminal report comes in relating to a money laundering case it is retained in SOCD until the criminal case is closed then archived.

6.47 Money Laundering high court cases (or any other high profile cases) are retained at Crown Office for 10 years then sent to NRS.

6.48 Sheriff and Jury cases are retained for 10 years then destroyed, though any of particular historical interest may be retained and sent to NRS.

SCDEA Proactive Intelligence led Investigations

6.49 Those cases which do not result in prosecution to be destroyed after 8 years.

Restraint and Confiscation Cases

6.50 When the accused is acquitted at court, the case is either closed or referred to CRU who will retain SOCD papers until case is finished. CRU will archive the papers.

6.51 When a confiscation order is made it remains open until order is paid in full and restraint order is recalled before going to the NRS. Papers should be weeded out before being sent to Archives, with only relevant court papers being retained. Copy productions will not be kept for permanent preservation.

6.52 The papers should then be kept for a minimum of five years after the date of right of appeal has lapsed.

6.53 Papers should then be destroyed or retained for a further 5 years and then sent to the NRS to be retained for historical interest.

SLAB

6.54 Reports are now generally sent directly to the relevant Procurator Fiscal's office. However, for those cases which are sent to NCD, the procedure is:

- Case folders relating to solicitors are retained for 10 years and then destroyed
- All other cases are destroyed after 3 – 5 years, depending on individual circumstances

Sequestrations

6.55 SOCD act as a post box for cases reported by the Accountant in Bankruptcy. The original report is forwarded to the Fiscal in the area where the offence has been committed. These cases are monitored in SOCD and instructions sought from the ADs or Lord Advocate. When the final disposal has been obtained they are closed off and stored in the basement at Crown Office.

6.56 Retain for 3 to 5 years then destroy.

SOCD Reported Cases

6.57 See Sequestrations

6.58 Retain for 3 to 5 years then destroy

CIVIL RECOVERY UNIT

Civil cases

6.59 For civil recovery cases in the Court of Session all files should be retained for a minimum of five years from the conclusion of the case. The date of conclusion of a case is for these purposes the date on which the period for the exercise of any right of appeal has expired following the conclusion of court proceedings arising from the case or the date on which a decision is taken not to raise such proceedings.

6.60 Where a case has been referred by National Casework Division CRU will retain the SOCD file and any productions that they have requested with their papers on conclusion of the case. CRU will inform National Casework Division on conclusion of their case in order that SOCD can update their systems and dispose of any productions that CRU have not requested.

6.61 Where a case referred to CRU by SOCD has been accepted and then found to be unsuitable for civil recovery purposes or for referral to another agency, then the file and productions will be returned to SOCD.

6.62 Where a case has been referred to CRU by SOCD but after investigation it is referred to the Asset Recovery Agency (ARA), CRU will retain the SOCD file and any productions requested from SOCD for a period of five years from the date of referral. CRU will inform SOCD that CRU case has been concluded when the case has been referred to ARA.

Cash cases

6.63 For cash cases all documents will be placed in electronic files and thereafter hard copies will be kept for no more than six months after the date of last activity on the file. Electronic copies will be kept for 12 years from the date of last activity on the file.

6.64 Where a cash seizure case has been referred to CRU by SOCD, CRU will retain the cash seizure file and the SOCD file for five years from conclusion of the case. The date of conclusion of a case is as stated for civil recovery cases.

Retention of case records for the Scottish Criminal Cases Review Commission (SCCRC)

6.65 The SCCRC will contact the Appeals Unit in Crown Office when they are considering an application and ask that case papers/records are retained

pending the outcome of the investigation. The Appeals Unit will write out to offices asking them to retain papers.

6.66 When the SCCRC advise the Appeals Unit that their investigation has concluded and that the case will not be the subject of any referral to the High Court, it is highly unlikely that the Commission will require any further information from the Crown. However, it is open to the applicant to re-apply to the Commission on different grounds. Against that possibility offices are requested to keep papers to hand for a period of 6 months. Thereafter, papers can be returned to filing, with the appropriate retention period for the level of the case being adopted from the date of return.

6.67 If the papers are requested again, the retention period will start afresh from the closure of the file.

6.68 If the case is held solely in electronic form, it will be retained in that format for the appropriate period.

6.69 **Electronic Data Retention Policy – identification of cases to purge**

Revised and simplified criteria – conservative purging policy means that there is no need to treat sexual cases separately.

NB Cases should be identified in the order given in this paper. In particular, the identification of cases as High Court, S&J, summary, direct measures and no action needs to be carried out in order since the criteria for later classifications depend on the result of the earlier classification.

1. Criminal Allegations Against Police – All CAP cases would be purged after 5 years. If a CAP leads to a criminal case, the criminal case would be subject to the same purge policy as all other criminal cases.

Criteria
Case status=closed (both CASZ.STAT and the latest CASE_STATUS.CASE_STATUS are "C")
Case category=CM (Complaint against police) or CW (complaint against prison officer)
Last closure date at least 5 years prior to today's date

Classification and purge instructions
Classify case as CAP

Purge and anonymise cases classified as CAP

2 Deaths - All Death records should be kept for 5 years. FAIs are part of normal Death records on the system. These are not treated as separate cases in the system so will be kept for the 5 years.

Criteria
Case status=closed (both CASZ.STAT and the latest CASE_STATUS.CASE_STATUS are "C")
Case category=DE (Deaths) or DM (Deaths military)
Last closure date at least 5 years prior to today's date

Classification and purge instructions
Classify case as Death

Purge and anonymise cases classified as Death

3 Advice and Direction - Advice and direction - purged after 5 years.

Criteria

Case status=closed (both CASZ.STAT and the latest CASE_STATUS.CASE_STATUS are "C")
Case category=AD (Advice and direction – sexual) or OR (Advice and direction – non sexual)
Last closure date at least 5 years prior to today's date

Classification and purge instructions
Classify case as A&D

Purge and anonymise cases classified as A&D

4. High court cases – these will not be purged

Criteria
Case status=closed (both CASZ.STAT and the latest CASE_STATUS.CASE_STATUS are "C")
Case category=criminal (see below for definition)

((Any marking for any subject is PEHC)
OR
(Any service record has a service type of IH (indict HC), RH (re-indict HC), ID (Indict), or RI (Re-indict))
OR
((Any marking for any subject is PE or PW) AND (no marking for any subject is PEHC, PESJ, PSJR)))

Classification and purge instructions
Classify case as High Court

Do not purge.

5. Sheriff and Jury - purge after 10 years

Criteria
Case status=closed (both CASZ.STAT and the latest CASE_STATUS.CASE_STATUS are "C")
Case category=criminal (see below)
Not previously classified as an HC case as per section 4 above.

((Any marking for any subject is PESJ, PEJR)
OR
(Any service record has a service type of IS (indict S&J), RS (re-indict S&J))

Classification and purge instructions
Classify case as S&J

Purge and anonymise cases classified as S&J if after 10 years from last date of closure

6. Summary Cases - purge after 5 years

Criteria
Case status=closed (both CASZ.STAT and the latest CASE_STATUS.CASE_STATUS are "C")
Case category=criminal (see below)
Not previously identified as an HC or an S&J case as per sections 4 and 5.
Any marking for any subject in case has marking procedure =summary

Classification and purge instructions
Classify case as Summary

Purge and anonymise summary cases if after 5 years from last date of closure

7. Non Court (Direct Measures) Cases – purged after 4 years.

Criteria
Case status=closed (both CASZ.STAT and the latest CASE_STATUS.CASE_STATUS are "C")
Case category=criminal (see below)
Not previously identified as an HC, S&J or summary case as per section 4, 5 and 6 above
Any marking for any subject in case is for a Direct Measure (see below for definition).

Classification and purge instructions
Classify case as Direct Measures

Purge and anonymise Direct Measure cases if after 4 years from last date of closure

8. No Action – purge after 2 years, unless case contains a serious charge (precautionary condition so as not to purge serious cases especially rape which may have been no actioned in error).

Criteria
Case status=closed (both CASZ.STAT and the latest CASE_STATUS.CASE_STATUS are "C")
Case category=criminal (see below)
Last closure date at least 2 years prior to today's date
Not previously identified as an HC, S&J, summary or Direct Measures case as per section 4, 5, 6 and 7 above

All subjects in case have a last marking with procedure NPRO or NFUR[1] (applied incorrectly) or a last marking of JUVI or PUPA .
No charge in the case is classified as FOS type 10.

Classification and purge instructions
Classify case as No Action

Purge and anonymise all cases classified as No Action

Definitions

Last closure date = the most recent of CASZ.CLOSED_DATE and CASE_STATUS.STATUS_DATE.
If CASZ.CLOSED_DATE is blank, use CASE_STATUS.STATUS_DATE.

NB Last closure date is only defined if both CASZ.STAT and the latest CASE_STATUS.CASE_STATUS are "C"

Direct Measure markings – Procedure of COFF, COFP, COMB, COMP, ALTF or markings of PD, PDID, DV, SDID, WL, RP

Criminal cases – case category of CD, CL, CO, CP, DA, DF, DS, FD, PA, PD, RI, RT, SP, ST, VE, WT

MIU
February 2014

[1] If a case is classified as No action in section 8 because a subject has a marking procedure of NFUR, the marking must have been applied incorrectly. If it had been applied correctly the case would have been identified in an earlier section according to the action originally initiated.

Chapter 7 - MANAGEMENT OF NON-CASE RELATED RECORDS

Electronic Records

7.1 The majority of COPFS business is now carried out electronically, rather than by way of paper. Most of the information produced is case-related, and so we have adopted a case management system, rather than a specific electronic records and management system for all electronic records generated and received by the Service. We also continue to receive a significant proportion of hard copy papers. Therefore, non-case related records are kept in a combination of electronic and paper systems which are appropriate to the type of information being retained.

7.2 Responsibility for the management of non-case related records currently rests with Federation Heads/Heads of Divisions and their respective Business Managers.

7.3 However, there are universal standards for records management and a records management policy for non-case related papers has been established which takes these into consideration.

7.4 The Service holds a significant amount of 'corporate' knowledge, for example information about our business functions, which may ultimately be worthy of permanent value and of interest to the people of Scotland and beyond. Once we no longer require this information for our own business needs this could be made available to the National Records of Scotland (NRS). The following is a list of the type of information which may be considered to be of permanent value:-

- Records relating to the origins and history of COPFS
- Annual and major reports
- Policy documents, relating to preparation of legislation, submissions to Ministers and senior officials
- Records relating to the implementation and interpretation of policy and to changes in policy
- Record sets of minutes and papers of major COPFS bodies
- Records relating to COPFS accomplishments, or to obsolete activities or investigations or aborted schemes initiated by COPFS
- Documents cited in or noted as having been consulted in the preparation of official histories
- Evidence of statutory rights or obligations, title to property, claims for compensation not subject to a time limit, and formal instruments such as awards, schemes, orders and sanctions
- Records which must be permanently preserved by statute
- Documents relating to well-known public or international events, persons or causes celebre, or major events which give rise to interest

or controversy at national level, particularly where those records add significantly to what is already known.
- Records relating to trends or developments in political, social, economic or other fields, particularly where they contain unpublished statistical or financial data covering a long period of time or a wide area

7.5 While much of this information is likely to be held centrally at Crown Office, PF offices should also be aware of the categories.

7.6 If offices consider that they hold information which should be transferred to NRS for permanent preservation, they should contact the Records Manager at Crown Office in the first instance.

7.7 It is also recognised, however, that in Procurator Fiscal Offices, and to some extent within Crown Office, the majority of non-case related information which is held is generally of a transitory nature, for example general office management functions, desk instructions, staff and court rotas, annual leave records etc. This type of information can be retained in shared electronic common folders, which must be reviewed on an annual basis to ensure that they are kept up to date.

Storing documents in electronic common folders

7.8 The guidance below is based upon a model which has been produced by Policy Division and is currently being piloted. It is recommended that other staff adopt these procedures for management of documents in common folders. A copy of the Policy Division Policy is attached at Annex 4

7.9 These folders can be set up depending on the topic or nature of the business contained within them, for example staff matters, accounts, rotas, policy issues. Access will be set up for individual teams, offices, functions or individuals from a number of offices who are involved in a particular departmental project.

7.10 These common folders will be stored on the appropriate drive and access will be limited only to those staff entitled to view and action the material stored therein.

7.11 Individual members of staff must be identified to maintain, review and delete electronic folders as required. The identified staff must maintain a record with the common folder of all deleted folders for audit purposes.

7.12 As a general rule, all documents should be saved into the relevant folder on the appropriate drive and not be password protected. The principal exceptions to this rule are documents that it would be inappropriate for all members of staff to have access to (eg documents that carry a protective marking of 'Restricted – Staff')

7.13 Electronic folders stored under the name of an individual member of staff should be avoided. Folders must be created under a topic, not the name of the person responsible for a portfolio. This will ensure that other staff are able to access the material when required.

7.14 When working on a document, the draft should be created and worked on in the common folder. Only the most up to date version should be stored there. Previous drafts should be deleted to ensure that everyone is working from the most recent version. Where a corresponding hard copy file exists, each version should be retained on the file in date order.

Version Control

7.15 Some records, for example, reports and guidance, go through various drafting stages. Continued drafting and redrafting of records can often lead to confusion over which draft is the current version. In order to manage the different versions of a record, staff should use version control.

7.16 Unnecessary duplication of records and information and lack of version control risks decisions being made on inaccurate or out of date information. It is essential to ensure that the current master version is identified and maintained in a shared common folder.

7.17 Unique version identifiers should be used to distinguish between different drafts and final versions and highlight when a record has become the final version.

7.18 For example, the first draft would be Draft (name of document) v0.1, then the second version would be v0.2 and so on.

7.19 Once the document had moved to a final version, it would become (name of document) Version 1.0. If minor revisions were subsequently required, then it would become Version 1.1 etc. Minor changes would involve small changes to the wording, for example, to clarify any misunderstanding about what was envisaged.

7.20 If major changes were required, a second final version would become (name of document) Version 2.0. A major change would involve any change to policy or practice. This may involve revision of a small section or the whole of the document.

7.210 Business Managers have responsibility for implementing this procedure in their own areas, and delegating responsibility for records management to named individuals in order to ensure consistency is maintained.

Naming Conventions for Electronic Documents

7.22 Documents must be filed within the folders/sub-folders with an easily identifiable heading. It should be immediately clear to anyone searching the system what a document is about without having to open it. This may mean that lengthy headings could be required. However, staff should bear in mind that the full pathname of the file should be no longer that 218 characters, otherwise difficulties may be caused in moving files from one area to another.

7.23 Staff should place the date of the document at the beginning of the heading, typing the year first, followed by the month, and then the day of the month as this keeps documents in date order and helps with the long term storage of documents.

For example,

2012.01.05 Reply.Jones to Smith.

2013.04.29 Email.Stewart to Jones

2013.06.11 Briefing min.Thomson to Anderson

2013.08.05 Agenda (Filed under the specific meeting sub-folder)

2013.10.10 Minutes (filed under the specific meeting sub-folder)

Naming Documents – Using Footers

7.24 Documents saved into shared folders should have a footer that describes exactly where the electronic version of the document can be found. The footer should be included in the 'footer' section of the document and should be made up as follows:-

Name of Office/Division/Common or Name of Team/Name of Sub-folder/Title of Document/Date.

7.25 The document should then be saved into the relevant folder/sub-folder, with the description inserted into the 'Save As' box being identical to the title of the document as set out in the final section(s) of the footer.

7.26 Footers should be left justified and should state the date the document was created, with the year first.

7.27 Saving documents in this way ensures that:

- Anyone with a hard copy of a document can easily find the electronic version if they need to access it;
- Anyone can access a draft document, should the need arise

Review and Disposal of Electronic Records

7.28 Shared electronic files should be reviewed on a regular basis in the same way as paper files. Responsibility for reviewing a file will rest with the member of staff with lead responsibility for the subject matter or their successor. Where there is doubt about the retention period, this should be discussed with the Federation Business Manager/Head of Division in Crown Office.

7.29 A record must be retained of all electronic common folders which have been destroyed and the date the destruction took place.

7.30 It should be noted, however, that there are some particular issues which need to be taken into consideration when destroying electronic records. These include:

- More than one copy of an electronic document may exist
- Once authorisation to destroy the records has been obtained, all copies must be deleted
- The ability to cross-refer electronic records to paper counterparts is important so that the same action is taken with both sets of records
- The deletion of an electronic record is not the same as destroying a record. This is because electronic records may still be retrievable unless reformatting takes place
- The media the records are held on may affect the destruction process and therefore should be taken into consideration

7.31 It is recommended that staff consult BS EN 15713: information on the secure destruction of confidential material for details concerning destruction of different media and records with different security classifications.

7.32 See Chapter 7 for more guidance on managing your e-mails.

Principles for Good Filing Practice - Electronic

The basic rules for good filing practice are as follows:

DO

- Ensure the structure of the file series is simple and easily understood by all staff using it

- Ensure file titles accurately represent file contents, for easy identification of correct documents
- Creat**e** a file list to ensure that all files are recorded
- Set up review dates on the file list at the creation stage to ensure that the folder only contains relevant, live material
- Create archive folders and review regularly, deleting material no longer required
- Try to file documents as soon as possible after creation/receipt
- Use recognised naming conventions so that documents can be easily found.
- File attachments with the document they relate to
- Ensure each stage of a legislative process of a Bill has its own file
- Ensure that all relevant e-mails and electronically saved documents are retained within the common folder and not within personal mailboxes
- Only end of exchange e-mails should be kept, but ensure all threads are retained
- Set review date for no longer than 5 years after first document date
- Allocate review disposal to files on closure. This ensures files are not retained longer than necessary, identifies those for retention or archive and helps rationalise electronic storage space
- Regularly sift current files to weed out those which could become closed or destroyed

DON'T

- Use 'miscellaneous' or 'general' in file titles. This tells you nothing of the file contents
- File a document without giving it a name compliant with the agreed naming convention
- Begin a file with a document which refers to another document which is not on that file
- File duplicate copies on other files – otherwise staff may not be working from the most up to date copy
- Retain spent drafts
- Retain documents which require to be shared for business purposes in a personal folder
- Guess at where a document should be filed. Take time to read preceding correspondence to ensure that you have the right one. If in doubt, ask the advice of senior/more experienced colleagues
- File different strands of the same subject on the same file – give them different files

Paper Records

7.33 A 'shared recording keeping folder' can also be a paper file.

7.34 Where a paper file is required, all correspondence, including end of exchange e-mails, documents and papers in respect of a particular topic should be filed.

7.35 Papers will be stored in files which can be ordered from Office Depot. Teams may colour-coordinate files for individual topics if this assists their working practices.

Creation of Files

7.36 Each team is responsible for the creation of files relating to their own areas of work. Paper files will be opened by the administrative staff in each team. The admin staff will also be responsible for filing papers. Where a new theme is required, this will be agreed between the lead official and appropriate admin staff.

7.37 In general, individual members of staff have responsibility to ensure material is printed for filing where they are the lead official. That is where:

- The initial correspondence was generated by him/her (this will include the filing of any associated papers or replies)
- He/she is the main recipient of the correspondence
- He/she has lead responsibility for an issue and thus has overall responsibility for ensuring that any documents required for future reference are stored on an appropriate paper file

7.38 Printing of papers for the files must be duplex.

7.28 Each team will store files relating to their own topics in filing cabinets in close proximity to their area of work. When files are closed, they will be transferred to the appropriate storage facility.

7.39 Files will be given a number for identification, which will also be recorded on the File List. The numbering will be along the following lines:-

Office/Name of Team/Topic/Name of any Sub File/Number

File List

7.40 A full list of the paper files is to be made available to all staff involved in the particular area of work. This will be maintained by an identified member of staff.

7.41 If a file is taken out for more than 24 hours by the lead official who has responsibility for it, or is passed by the lead official to another member of staff, the admin member of staff who has been allocated responsibility must be advised so that the file location can be updated. When the file is returned, the admin staff must be advised so that the file list can be updated.

7.42 The file list will be reviewed on a regular basis, at least every year, by admin staff to ensure that all closed files have been recorded and that files due for review/transfer/destruction are dealt with accordingly. The person with lead responsibility for the subject matter will take the decision on whether a file required to be kept or can be destroyed.

7.43 It will be a specific objective for the identified staff to check the files on a regular monthly basis and to draw any files to the attention of lead officers which have not been added to for 6 months.

7.44 Closed files which have been filed in the appropriate storeroom will also be brought to the attention of lead officers on a regular basis for review.

7.45 It is important that files are reviewed at the appropriate stages. The lead official who has been working most closely on a topic has the most in depth knowledge of the subject matter. He/she is aware of the importance of specific material and political sensitivities. The lead official is therefore best placed to advise on closure of files and review of contents at an early stage, for example, after a policy has been implemented.

7.46 It will therefore be a specific objective for lead officials to review the contents and consider whether the file can be destroyed, is required for the future or should be transferred to NRS for permanent preservation.

7.47 When considering non-case related files which might be suitable for permanent preservation at NRS, contact should be made with the Records Manager in the first instance. The Records Manager will then liaise with officials at NRS and where appropriate arrange transfer of the files. It is likely that most files which are required for permanent preservation at NRS will have been created in Crown Office. However, Federation Business Managers should be alive to any files which are held their offices which might fall within the above categories.

Closed files

7.48 A file must be closed when:-

- 5 years have elapsed since the first paper
- Its subject matter is no longer current
- Papers have not been added for 1 year (unless the subject matter is such that papers will not be added regularly – eg biannual, annual meetings)
- It has become too bulky and a new part is required

Review of Files

7.49 Files must be reviewed on a regular basis – at least annually. Responsibility for reviewing files rests with the person who leads on the subject matter or their successor.

7.50 If it is clear at the time of closure that the file will no longer be required, it can be destroyed straightaway. Records must be kept of all files which have been destroyed.

7.51 The long term value of a file may not be clear until closure. In these circumstances, records should not be destroyed earlier than five years after the date of the last document.

7.52 Where a decision is not obvious either at creation or at the time the file is closed, the file may be marked for re-examination five years after its closure date. A disposal decision should be possible at this point.

7.53 Occasionally, and this should be very infrequently, a second review will be necessary and this is scheduled for up to 25 years after the date of the first document on the file. Files should only be retained after this time on the authority of the Federation a Business Manager/Head of Division in Crown Office.

Filing

Principles for Good Filing Practice - Paper

The basic rules for good filing practice are as follows:

DO

- Ensure the structure of the file series is simple and easily understood by all staff using it
- Ensure file titles accurately represent file contents, for easy identification of correct papers
- Always file reply on same file part as original document. The papers should be filed in the order in which they were written
- Try to file papers as soon as possible after receipt
- File papers in reverse book order so latest document is seen on opening cover
- File attachments below the document they relate to
- File bulky documents in pouches inside the file cover with brief description of contents
- Ensure each stage of the legislative process of a Bill has its own file
- File all papers on the right hand side of the file cover
- Print and add to the file all e-mails and electronically saved documents relevant to the ongoing story
- Papers for hard copy file must be printed on both sides

- Only end of exchange e-mails should be kept, but ensure all threads are retained
- Close files 5 years after first paper date. If file gets too large, and correspondence is still ongoing, open up a new part
- Allocate review disposal to files on closure. This ensures files are not retained longer than necessary, identifies those for retention or archive and helps rationalise storage space
- Regularly sift current files to weed out those which could become closed and stored centrally or destroyed
- Encourage use of a tracking system for transferring files to another official

DON'T

- Use 'miscellaneous' or 'general' in file titles. This tells you nothing of the file contents
- Store protectively marked files in open cupboards. Restricted files must be kept in cupboards to be locked at night and when the office is unmanned. Files with higher protective marking must be kept in secure cabinets to be locked at all times
- Remove papers from files. If absolutely necessary, then cross-refer on original file, or make copies for other files and replace the paper on the original file
- Begin a file with a paper referring to another paper which is not on that file
- File duplicate copies of the same paper, unless there are annotations which may be of future relevance
- File spent drafts
- Lock official papers in personal drawers
- Keep folders which contain the originals or the only copies of papers in personal drawers
- Guess at where a paper should be filed. Take time to read preceding correspondence to ensure that you have the right one. If in doubt, ask the advice of senior/more experienced colleagues who should be encouraged to annotate appropriate reference numbers to correspondence passed over for filing
- File different strands of the same subject on the same file – give them different files

8 MANAGING EMAIL

8.1 Email is a tool for written communication and has largely replaced the traditional paper correspondence or telephone call as the most used form of communication within COPFS. Emails need to be managed just like any other records we create.

8.2 All staff who create, receive and use records (including emails) have records management responsibilities. These can be summarised as a responsibility to create appropriate records, to capture important emails within your own area of work and record keeping system and to destroy those emails which are no longer needed.

8.3 Emails are legally admissible and may be disclosed under legislation such as the Data Protection Act 1998 (DPA) and the Freedom of Information (Scotland) Act 2002 (FOISA) or in a court of law. The DPA permits people to see emails that COPFS holds about them while FOISA gives people the right to access any other recorded information which we hold, including emails. The DPA also requires us to hold information about living identifiable individuals for no longer than is necessary, to ensure that information is accurate and to adopt appropriate security measures for this information to protect it from unauthorised access, amendment or deletion.

8.4 Before you send emails you should consider whether the content is accurate and appropriate. It is advisable to work on the assumption that all work emails you create could be accessible to somebody and may require to be released under the DPA or FOISA.

8.5 The keeping of electronic records, including emails, incurs large storage and maintenance costs. As a result of this, ISD have advised that all mail older than 8 weeks contained in individual 'Sent Items' folders will be automatically deleted when Outlook is closed. Staff are therefore required to manage their mailboxes in such a way as to avoid important information being lost.

8.6 You should actively manage your inbox by disposing of emails as soon as they are no longer needed but you must ensure that emails which are required for business purposes are consistently captured and managed in a shared record keeping folder outside of personal inboxes. This enables other staff to access information for business continuity purposes or answer a request for information within the statutory timescales in your absence. If copying/moving emails that are over 60 days old to other mailboxes or shared drives, staff need to ensure that the full (unarchived) version is copied and not the archived shortcut. Advice on working with archived messages can be found on PF Eye.

8.7 It is important that all information in relation to a particular topic is retained in the one place which is easily accessible. It is difficult, hugely

costly and time-consuming to retrieve e-mails which have been stored in personal folders, on laptops, discs or even home computers.

8.8 Emails are not private or confidential and can be illegally intercepted. It is the responsibility of all members of staff to consider the appropriateness of using e-mail to discuss sensitive subjects. Staff must not exchange case-related information by e-mail unless through the Criminal Justice Secure Mail Scheme. (insert link -http://www.cjsm.cjit.gov.uk/what/index.php) Further information on Information Security is contained in Chapter 8 of this manual.

8.9 At the start of the email, explain whether it is for information or action and ensure that its purpose and content are clearly explained. This helps receivers to identify, prioritise and retrieve e-mails more effectively. Make it easy to respond to your message by clearly identifying (eg by numbering) your questions/requests.

8.10 Try to restrict an email to one topic, and do not mix personal and work matters together.

8.11 When sending an attachment with the email to an external stakeholder or member of the public, you should normally send a pdf version, rather than a word document so that there is no risk of it being altered on receipt.

8.12 Before staff transfer to another post or leave COPFS they should discuss their email management with their line manager to ensure that all relevant emails are captured in an appropriate shared electronic/paper folder which will be easily accessible by the remaining members of staff in the team/office.

Managing Emails – Do's and Don'ts

Do:

- Remember that all work emails are COPFS records
- Exercise the same degree of care and professionalism with regard to the content of email messages as you would with a letter or memo
- Set an out of office message giving alternative contact details when you are away, or arrange for someone else to check your email
- File important emails so that they are accessible to other people on a common folder
- Delete unwanted emails as soon as they are no longer required
- Send pdf attachments rather than Word documents to external contacts
- Make use of expiry date and properties options
- Use short meaningful titles/subjects for your emails
- When replying to an email, keep the original text as part of your response

- Remember that email is not a secure form of communication and use secure email for sensitive communication
- Remember that all your emails may be open to scrutiny

Don't

- Keep the only copy of important emails in your in and sent items boxes
- Allow backlogs of unwanted emails to accumulate in your account
- Copy emails to people unless they need to see them
- Mix personal and work emails
- Address more than one topic in one email
- Annotate or change the text of the original -mail when replying to it
- Use a non-COPFS email account for COPFS business
- Use symbols in the subject line of emails
- Use your Deleted Items and Sent Items folders to store items you want to keep
- Have a large number of unread items in your mailbox as these will not be archived. Archiving reduces the space used by your mailbox

NB Staff must ensure that they also adhere to the Acceptable Use Policy.

Chapter 9 - SECURITY CONSIDERATIONS

9.1 The management of the security of information and records is essential to protect the information assets of COPFS and criminal justice partners and stakeholders. We must ensure business continuity, minimise risk and protect the rights of individuals about whom we hold information.

9.2 Staff should be aware of potential risks that exist in what may be perceived as a secure internal environment, particularly where sensitive business and personal information is used and stored.

9.3 It is essential to ensure the authenticity, confidentiality, context, integrity, reliability, structure and usability of records and information held in all media and formats.

9.4 COPFS must ensure that records are easy to retrieve, protected from deterioration/damage and unauthorised access.

9.5 Consideration must be given to storage of paper records to ensure that they are not subject to theft, unauthorised access, or accidental damage from fire or water, vermin or mould.

9.6 Staff and local managers should have regard to the following issues:-

- Security measures are put in place to restrict access by unauthorised persons including regulating who is permitted access to records and record storage areas and in what circumstances

- Paper records are stored in appropriately secure lockable filing equipment and storage facilities to which access is controlled

- Staff should pay particular attention to the Departmental Security Guidance and the Acceptable Computer Use Policy

- Staff should never tell anyone their password. It should not be written down and left for others to see

- If staff log on accidentally to an inappropriate internet site, they should log off immediately and inform their line manager as soon as possible. Access and attempted access to inappropriate sites is continually monitored

- Staff should never send inappropriate email. If anything inappropriate or offensive is received, staff should inform their line manager, Help Desk or Departmental Security Officer

- Computer screens should not be left as readable when staff are absent from their desk or work area. Use the CTRL+ALT+DEL keys and then select the option to Lock Computer

- Computer users should log out when absent from their desks for lengthy periods

- Staff must be aware of the security risks associated with capturing electronic documents from other systems into COPFS systems

- Staff must be aware of security risks to records and equipment whilst working in public areas and when working at home, or away from the office

- Sensitive documents/papers should never be taken out without authorisation. Details should be logged including who has taken the documents and the reasons for removal and for how long

9.7 Security Guidance is available to staff on PF Eye under the Staff Information section and provides valuable advice. Sections which are particularly relevant to the issue of records management are highlighted below.

9.8 The COPFS Information Security Policy of COPFS serves to ensure that;

- Information will be protected against unauthorised access;

- Confidentiality of information will be assured;

- Integrity of information will be maintained;

- Information will be available to authorised personnel as and when required;

- Regulatory and legislative requirements will be met;

- Business Continuity Plans will be produced, maintained and tested;

- Information security training will be available to all staff;

All breaches of information security, actual or suspected, will be reported to and investigated by the Departmental Security Officer.

9.9 It is important that all staff understand the principles of Document Security and exercise care in handling and protecting the confidentiality of sensitive material that comes into their possession in the course of their duties.

9.10 Sensitive documents, files, electronic material etc should be given a classification (or marking) to indicate its importance and how it should be handled. These markings are often seen on the top of documents. These markings are known as the Government Security Classifications and COPFS is required to comply with requirements.

9.11 We are currently operating with the old classifications of Not Protected, Protect, Restricted, Confidential, Secret and Top Secret in line with the Police but will move to the new classifications of Official, Official – Sensitive Secret and Top Secret as soon as practical.

9.12 Access to electronic cases which are particularly sensitive or have distressing content and associated documents are restricted to nominated members of staff only. This is done to protect the confidentiality of information in the relevant cases and protect members of staff from exposure to distressing details.

9.13 COPFS operates a clear desk policy. Staff should clear desks of case related and other sensitive material before going home or when away from their desks for long periods during the day.

9.14 Hard copy files containing case related and other sensitive material must be locked away at all times when not in use. The information contained within them must be protected at all times from unauthorised access and from the possibility of deliberate compromise or opportunist attack. When destruction of such records is required, it must be in a manner which makes reconstruction unlikely.

9.15 "Restricted" papers must be stored in normal, lockable containers. However, special security Cabinets can be provided to staff who hold Confidential, Secret and Top Secret material. Further information is available from the Departmental Security Officer.

9.16 Staff must ensure that protectively marked material, security keys as well as valuable portable assets are securely stored. Failure to do so constitutes a security breach. Security staff can carry out random 'out of hours' checks.

Exchanging Information

9.17 Staff must be aware of the need to protect the exchange of information through the use of computers, telephones, mobile phones, answer machines, faxes, video communications etc. Exchange of case-related information by e-mail must be through the Criminal Justice Secure Mail or through the Secure Disclosure Website.

9.18 Staff should not store personal or restricted data on the C drive of their laptop unless it is stored in the encrypted 'Offline Files' working area, nor should they store personal or restricted data on any unencrypted removable media.

9.19 It is the responsibility of staff entrusted with valuable portable equipment, such as laptops, TVs, videos, mobile telephones, Blackberry devices etc to ensure that they follow the advice provided on security procedures to help protect the equipment from theft.

9.20 You should ensure that the laptop is locked down when not in use. You should not carry all the components together in the same bag. Similarly the PIN number should be kept secure and never divulged to anyone.

9.21 Line managers also have an essential role to play in ensuring that security procedures are followed and COPFS assets under their control are adequately protected. Particular attention should be drawn to the need to hold the relevant details, such as make, model and serial number of all their portable valuable equipment, which in the event of theft or loss are required for inclusion in the necessary report to the police.

Further guidance from The Bulletin April 2015 is attached at Annex 5.

Chapter 10 - NATIONAL RECORDS OF SCOTLAND

Introduction

10.1 The National Records of Scotland (NRS) is the main repository for the public and legal records of Scotland which have been identified as being worthy of permanent preservation. It also advises the Scottish Government, amongst others, on the care of their records. COPFS files which are chosen for preservation on the basis that they are of historical interest, based on criteria set out by NRS are transferred to NRS's custody and held there on our behalf. Criminal case files and Fatal Accident Inquiry (FAI) papers are transferred after a period of ten years from the date of the last action on file. Selected administrative files are also transferred, sometimes at an earlier stage.

10.2 The main points of contact for NRS are through the Response and Information Unit, Policy Division, Crown Office, High Court Registry, Crown Office and through Dumbarton Disposals. These Units are in regular discussion about case paper policy and transfer of case-related and policy files.

Requirements under Freedom of Information and Data Protection Legislation

10.3 Since January 2005, under the Freedom of Information (Scotland) Act 2002 (FOISA), individuals have a greater right of access to information held by public authorities. The legislation states that "a person who requests information from a Scottish public authority which holds it is entitled to be given it by the authority". This means that even restricted information which is held at NRS on behalf of COPFS can now be made available to the public, subject to the application of any appropriate exemptions which may necessarily restrict access.

10.4 The general rule is now that records transferred to NRS should be considered open unless specific exemptions are applied.

10.5 COPFS files, which relate to criminal prosecutions, sudden deaths and fatal accident inquiries, often contain material which is of a sensitive, confidential and, at times, distressing nature. Therefore it is appropriate for COPFS papers not to be readily available in the public domain as soon as they are transferred to NRS. This protects the individuals whose personal details are contained in the papers as well as members of the public.

10.6 COPFS papers held by NRS remain restricted, as certain exemptions under the legislation attract a longer closure period. For example, the Act

exempts for a period of 100 years the release of a deceased person's health record, or papers held by a public authority in relation to an investigation by virtue of a duty to ascertain the cause of death of a person. In some cases, the Data Protection Act 1998 also applies, restricting access to particular types of information about living individuals.

10.7 It has therefore been agreed that when NRS receive a request to review COPFS case files which are less than 100 years old, the requestor will be referred to the Response and Information Unit, Policy Division in the first instance so that a review can be carried out to see what information might be released and considered "open" for subsequent viewers.

10.8 It should be noted that the trend is increasingly towards closing records containing sensitive personal data for 100 years, rather than for 75 years, which was previously more generally the case. This is largely to do with (a) lengthening lifespans, which make it increasingly likely that an adult could still be alive 75 years after the date of a case and (b) there is a very good chance that anyone who was a child at the time of a case will still be alive 75 years later. Each case must be considered on its own merits, however, and there could be some circumstances where it may be appropriate to open a deceased person's health record before 100 years has passed.

Special Handling Procedures

10.9 Records will only be retransmitted by NRS to three units within Crown Office:

- Response and Information Unit, Policy Division,
- High Court Registry and
- Appeals Unit administrative staff

10.10 These units will log the receipt of the archived files and take responsibility for ensuring that they are returned timeously when they are no longer required.

10.11 When records are re-transmitted from NRS, either for review as set out above, or for some other business purpose, such as the commencement of an appeal, special handling procedures apply.

10.12 Handling archive material affects its life expectancy. All archive material which is temporarily retransmitted for business purposes must be handled with special care to ensure its survival for future generations.

10.13 A note from NRS will accompany any retransmitted file setting out the appropriate handling procedures and this must be observed by staff. In essence it states:

- Make sure that your hands are clean
- Use only pencil when taking notes from the files
- Do not eat, drink or smoke near the files
- Use only acid free bookmarks (provided). Do not use post-it notes as markers
- Do not remove documents from a bundle or file
- Do not add documents to a bundle or file (see COPFS desk instructions for how to deal with additional papers relating to an archive file)
- Do not mark the documents in any way. Never employ correction fluid on an original document*
- Be careful and vigilant when making photocopies from documents, especially when these are in files. Rough handling can cause documents to become loose and may lead to them becoming lost or misplaced
- Ensure that files are properly stored in a secure and risk free environment (eg not near sources of water or extreme temperature)
- Return this file to NRS as soon as you have finished with it

*NB: where data protection requires a redaction exercise to protect individuals named in a file which is to be made available for inspection, a photocopy must be used for this purpose. *The original document must not be marked or changed in any way.*

New records for association with archive file

10.14 In particular, staff must not add any new papers to the archive file. In appropriate circumstances, Response and Information Unit, Registry or Appeals in Crown Office will supply staff with an appropriate folder and instructions for the filing of new papers.

Annex 1

GUIDANCE ON WHAT REQUIRES TO BE KEPT WHEN CASES ARE WEEDED AND IN WHAT ORDER

Summary Cases:-

1 Court minutes
2 Copy complaint
3 Custody statements (applicable)
4 SPR
5 Witness statements (original)
6 Witness statements (redacted)
7 Minute of Agreements
8. Bail appeal report (if applicable)
9 Correspondence file (most recent correspondence on top)

Sheriff & Jury Cases:-

1 Precognition backing sheet which includes minutes
2 Precognition
3 Minute sheets
4 Section 76 Indictment (if applicable
5 Indictment (if more than one version then one of each)
6 Section 67 notices
7 Copy of execution 67 notice
8 Petition
9 Custody statements
10 SPR
11 Witness statements (original)
12 Witness statements (redacted/disclosure)
13 Crown Counsel's instruction
14 Section 76 report (if applicable)
15 Minutes of agreement
16 Bail Appeal report (if applicable)
17 Transcripts of Judicial Examination (if applicable)
18 Transcripts of Police interview tape (if applicable)
19 Copy Documentary productions
20 Copy of any photographs
21 Copy of any medical records
22 Correspondence file (most recent correspondence on top)

High Court Cases:-

1 Precognition backing sheet which includes minutes
2 Precognition
3 Minute sheets
4 AD notes
5 Section 76 Indictment (if applicable
6 Indictment (original and amended version(s))
7 Section 67 notices
8 Copy of execution 67 notice
9 Petition
10 Custody statements
11 SPR
12 Witness statements (original)
13 Witness statements (redacted/disclosure)
14 Crown Counsel's instruction
15 Section 76 report (if applicable)
16 Minutes of agreement
17 Bail Appeal report (if applicable)
18 Transcripts of Judicial Examination (applicable)
19 Transcripts of Police interview tape (applicable)
20 Copy Documentary productions
21 Copy of any photographs
22 Copy of any medical records
23 Correspondence file (most recent correspondence on top)

Routine Death Cases:-

1 Minute backing sheet
2 F5 Notification of Death
3 Police/Death report
4 Notification to Registrar
5 Correspondence File (most recent correspondence on top)

Investigated Death Cases:-

1 Minute backing sheet
2 F5 Notification of Death
3 Police/Death report
4 Post Mortem report
5 Toxicology report (if applicable)
6 Histology report (if applicable)
7 Witness statements (original)
8 Witness statements (redacted/disclosed) (if applicable)
9 Precognition (if applicable)
10 F11 Petition for FAI (if applicable)
11 Books of photographs
12 Copy of documentary productions

13 Correspondence file (most recent correspondence on top)

Complaints Against Police Cases (No Proceedings):-

1 Police report
2 Witness statements (original)
3 Correspondence file

Complaints Against Police Cases (Summary Proceedings):-

1 Court minutes
2 Copy complaint
3 Police report
4 Witness statements (original)
5 Witness statements (redacted)
6 Minute of Agreements
7 Correspondence file (most recent correspondence on top)

Complaints Against Police Cases (Solemn Proceedings):-

1 Precognition backing sheet which includes minutes
2 Precognition
3 Minute sheets
4 Section 76 Indictment (if applicable
5 Indictment (if more than one version then one of each)
6 Section 67 notices
7 Copy of execution 67 notice
8 Petition
9 Police report
10 Witness statements (original)
11 Witness statements (redacted/disclosure)
12 Crown Counsel's instruction
13 Section 76 report (if applicable)
14 Minutes of agreement
15 Transcripts of Judicial Examination (applicable)
16 Transcripts of Police interview tape (applicable)
17 Copy Documentary productions
18 Copy of any photographs
19 Copy of any medical records
20 Correspondence file (most recent correspondence on top)

ANNEX 2

Policy Electronic
Filing Guidance 2015

ANNEX 3

PROMIS

PROMIS is the COPFS database. It contains information about subjects reported by the police and other agencies. These reports may have been received electronically from the police or come in hard copy e.g. TV licensing offence reports.

Any hard copy reports have to be manually put on to the PROMIS database. PROMIS contains criminal cases, deaths and occurrence reports etc. The PROMIS database contains information about the subject, such as, in a criminal case, the subject name and address, the charges, witnesses details, and a list of all cases reported against the subject, i.e. the soundex.

PROMIS interfaces with a number of other systems. These IT systems are external to COPFS.

POLIN – Electronic Documents

This is the data transfer line or "link" between the COPFS database and the police (and any other reporting Agency which comes on line). It allows the police to send their reports electronically and for COPFS to communicate with the police by sending and receiving e-mailed documents created on our PROMIS database.

COPLINK

The PROMIS database interfaces with both the Sheriff Clerk's and some District Court Clerk's computer databases. The Sheriff Clerk's database is called COP. The "link" between the COPFS and the Clerks is called COPLINK. PROMIS sends initial court appearances to the Clerk via COPLINK. Once the case has called in court the Clerk will update their COP database and will send the court results back to COPFS PROMIS database using COPLINK.

SOS-R

SOS-R is the forerunner to FOS and is a computer software package. It pulls information from PROMIS and puts that information into templates/style letters. For example, a citation kit is a template that pulls details about the

accused, the charges, the marking and court appearance and puts them into the citation kit.

Anything that is not processed in FOS can be located on SOS-R, as well as some cases that are processed using FOS. The data can be viewed in two ways:-

- By looking on the intranet under Quick Links for SOS – Area ** and choosing Document Maintenance. This will show the criminal cases and any further documents received from the police (eg full statements) and letters created by COPFS.

- To you can also access the case information by accessing the PROMIS icon on the desktop, where you can view what has happened to a case which is not processed using FOS.

FOS

The Future Office System (FOS) is the current software that provides COPFS with an easier way of displaying and changing information we store in our database i.e. accused (subject), witness, charge information etc. It also allows us to produce case documents in an easier way and introduces the concept of on-line case marking.

Full information about using the above systems is available in the Case Processing Manual.

Annex 4

COPFS Retention Schedules.xls

ANNEX 5

Guidance from The Bulletin 2015

We all share a responsibility to protect the security of the confidential and sensitive information COPFS holds about victims, witnesses and people accused of crime. All of us come into contact with sensitive material every day.

Our responsibilities stem not only from Government policy but are also legal obligations on us as individuals and on COPFS as an organisation. The legal obligations are set out in various statutes, particularly the Data Protection Act 1988

For all staff, compliance is obligatory, not optional. **All confidential and sensitive information, whether hard copy or electronic, must be handled and processed according to our obligations.**

The potential harm caused by the loss of confidential and sensitive information to members of the public – to whom we owe a duty of care – and the risk of reputational damage to COPFS is so serious that any breach of COPFS policy will require to be dealt with as a potential disciplinary matter.

The very real risks around breaches of security impact on all of us and our ability to prosecute crime and include:

Serious physical harm to the victims and witnesses named

- Potential for intimidation of victims and witnesses
- Potential for attempted extortion or corruption of those named in the lost information or the member of staff who has caused the loss
- Loss of public confidence and trust in COPFS
- Loss of trust in COPFS by our criminal justice partners
- Disciplinary investigation and potential disciplinary action for those staff involved
- Impact on colleagues arising from the need to investigate losses and the worry and concern this can cause
- The potential for statutory action from sources such as the Information Commissioner – other public sector organisations and firms conducting legal casework have been very heavily fined in similar circumstances

- The potential for job losses arising from any such large fines– COPFS would be liable and therefore the budgetary impact could be significant.

The current published security guidance is being updated in partnership with the Trades Unions and will be made available on the intranet in the near future. **Meanwhile all staff are urged to bear in the mind the following key points which will always apply on how to protect sensitive data and what is required of all of us, in and out of office:**

- **Sensitive data should never be disposed of in ordinary waste bins but in confidential waste bins**. The easiest way to ensure this is to put all paper into confidential waste bins.
- **Case files and other sensitive material must be stored in locked filing equipment** or other storage facilities to which access is controlled
- **Desks should be cleared of case-related and other sensitive material before going home or when away from desks** for long periods during the day
- **Never email any case or work-related information from your office to a home email account**
- **Staff must be aware of security risks to records and equipment when working in public areas or out of the office**

Actions out of Office

- Work on cases should normally be done in the office during working hours. **Sensitive data should never be taken out of the office, on paper or on encrypted pen drive or laptop, without receiving email authorisation from a manager.**
- **If case papers are being transported outwith a COPFS office it should be in a locked case.** If you don't have access to one, lockable cases can be provided for this purpose. If required, please contact the relevant Business Manager.
- Taking case papers home or on a journey is a risk and whenever possible should be avoided. **There are some documents such as productions and medical or social work records which should <u>never</u> be taken home.**
- If case documents have to be taken home, **it is less of a risk to use an encrypted laptop or pen drive than paper files**

- **Use a COPFS laptop when working remotely**, having downloaded case related or work material on to it in the office. The only exception which permits a home PC to be used for work on COPFS material is when you are working on a home PC with a COPFS encrypted pen drive as set out below.
- **If a COPFS laptop is unavailable, use a COPFS encrypted pen drive to carry information downloaded from our systems securely between the office and your home.** The data from the pen drive can be used simply and securely on your home PC by following the **published ISD guidance**. If you use the 'open' option on the pen drive, rather than 'extract' option, you will be able to open the documents to allow you to see them on your home PC screen whilst ensuring that any work on them remains encrypted and on the pen drive. If you extract the document from the pen drive it will be saved on the home PC and will no longer be secure.
- The use of only authorised COPFS laptops and pen drives for working on confidential and sensitive data ensures that all such material is properly destroyed when the equipment is taken out of commission. The same cannot be said with certainty when data is deleted from a home computer – *the data remains on the hard drive and may remain retrievable.*
- Staff should be aware of the **social media policy** and not use social media to comment on any COPFS issues or breach any confidentiality and it is strongly recommended that you do not identify the fact that you work for COPFS

Annex 6

GLOSSARY

Access – right, opportunity means of finding, using or retrieving information.

Accountability – principle that individuals, organisations and the community are responsible for their actions and may be required to explain them to others.

Business Classification Scheme – is based on the analysis of functions, processes and activities. It documents the structure of a records management system and the relationships between records and the activities that generate them. It provides an essential basis for the intellectual control of records and facilitates their management and use over time. A business classification scheme can be used to ensure that all records are stored consistently, regardless of their format and also underpins an Electronic Document and Records Management System (EDRMS)

Capture – refers to the actions that are taken to secure a record into an effective records management system, where the record can be maintained and made accessible for as long as it is needed.

Classification – systematic identification and arrangement of business activities and/or records into categories according to logically structured conventions, methods, and procedural rules represented in a Business Classification Scheme

Context – a record must be supported by information about the circumstances in which it was created and used. Records cannot be fully understood without adequate knowledge of the activity that gave rise to them, the wider function of which the activity forms part, and administrative context, including the identities and roles of the various participants in the activity. Contextual information must therefore be captured in the records themselves or in the systems that are used to maintain them.

Creation – refers to the creation of a record in a business activity.

Destruction – a process of eliminating or deleting, beyond a possible reconstruction.

Document – recorded information or object which can be treated as a unit.

Disposition – range of processes associated with implementing records retention, destruction or transfer decisions.

EDRMS – electronic document and records management system – a dedicated system for capturing records. It supports the capture, registration, storage and indexing, ownership and access rights, retrieval, checkout and return of documents and records.

Evidential value – the usefulness of records as the primary or legal evidence of an organisation's authority, functions, operations, transactions and basic decisions and procedures.

File list – list of files and their titles.

Filing – the process of sorting and arranging, classification or categorizing, and storing records so that they may be retrieved when needed.

Functions – things an organisation has to do to achieve its corporate goals and strategies.

Metadata – data describing context, content and structure of records and their management through time.

Migration – act of moving records from one system to another, with maintaining the records authenticity, integrity, reliability and usability.

Preservation – processes and operations involved in ensuring the technical and intellectual survival of authentic records through time.

Record – any recorded evidence of an activity.

Recordkeeping system – information system which captures, manages and provides access to records through time.

Records management – field of management responsible for the efficient systematic control of the creation, receipt, maintenance, use and disposition of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records.

Records series – a group of related records or documents that are normally used and filed as a unit because they result from the same activity or function or have some relationship arising from their creation, receipt etc, and that permit evaluation as a unit for retention scheduling purposes.

Retention period – the length of time particular records must be kept. This is usually expressed in terms of years or months.

Retention schedule – documents how long records are retained for, how and where they should be stored and what action needs to be taken once the record reaches its retention date.

Retrieval – the process of locating and withdrawing records and delivering them for use.

Tracking – creating, capturing and maintaining information about the movement and use of records.

Transfer – (custody) change of custody, ownership and/or responsibilities for records.

Transfer (movement) moving records from one location to another.

Version control – the management of multiple revisions to the same document. Version control enables us to tell one version of a document from another.