Information and Records Management Handbook

Scottish Information
Commissioner

Contents

Glossary and abbreviations

Term used	Explanation
EIRS	Environmental Information (Scotland) Regulations 2004
FOISA	Freedom of Information (Scotland) Act 2002
Commissioner	The Scottish Information Commissioner
DPA	Data Protection Act 2018
HOCS	Head of Corporate Services
HOE	Head of Enforcement
HOPI	Head of Policy & Information
HOD	Head of Department
FAM	Finance and Administration Manager
CST	Corporate Services Team
IRM	Information and records management
ICT Systems	The term ICT systems refers to all: • Hardware e.g. desktops, laptops, mobile phones and memory sticks • Software used by these systems e.g. Microsoft Outlook Email Client, Internet Explorer, Virtual Cabinet • Drives located on the servers and individual computers
IT Account	Password secured account set up by CST allowing a staff member access to the Commissioner's computer systems (as detailed above)
VC	Virtual Cabinet
UK GDPR	UK General Data Protection Regulation

Section 1 – Introduction, Scope and Responsibilities

Introduction

1. The Scottish Information Commissioner's ('the Commissioner's') Information and Records Management Policy (IRM Policy) is supported by this handbook which details procedures and guidance for staff on information and records management and the use of all of the Commissioner's ICT systems, which you must adhere to.

2. The key purpose of the Information and Records Management Handbook (the IRM Handbook) is to ensure that:

   - you are aware of the Commissioner's procedures and guidance for information and records management
   - you apply the Commissioner's procedures and follow the guidance for information and records management consistently.
   - you are aware of the controls in place to manage and maintain the security of systems
   - you apply the controls in place to manage and maintain the security of systems consistently and in accordance with the related requirements

3. For business continuity purposes, it may be necessary to provide temporary and interim policies and procedures to add to or amend the provisions set out in this handbook, for example, when dealing with the impact of a pandemic. Staff will be advised where such temporary and/or interim policies and/or procedures are required and the reasons for them.

Scope

4. The records management system in our organisation is made up of:

   - the IRM Policy
   - the IRM Handbook
   - the File Plan and Retention Schedule
   - the Records Review Procedures
   - Key Document Handbook
   - Register of Key Documents
   - related policies and procedures and guidance - there are several policies and procedures whose main subject is not records management but which stipulate records management requirements specific to that subject, for example, the Investigations Handbook, the Data Protection Policy and Handbook and the Employee Handbook.

5. The IRM Handbook applies to:

- Every member of the Commissioner’s staff including permanent, temporary and fixed term employees and employees who are on secondment with the Commissioner during the course of their employment with the Commissioner
- all contractors and agents who, at any time, use or may have access to the Commissioner’s internet, email and other business communications systems during the course of their business with the Commissioner
- any other person authorised to access the Commissioner’s business and/or ICT systems.

Responsibilities

6. It is your responsibility to comply with guidance, advice and procedures set out in the IRM Handbook. You must ensure that you are familiar with the contents of the IRM documents and, also, the contents of any related procedures and guidance. You will be asked to confirm that you have read and understand the IRM Policy and the IRM Handbook on an annual basis.

7. Under section 45 of FOISA you are subject to a duty to keep confidential information that is provided to the Commissioner to carry out our functions under FOISA and the EIRs, and may only disclose it with lawful authority.

8. Under section 65 of FOISA it is a criminal offence for a Scottish public authority (or for any person employed by, who is an officer of, or is subject to the direction of, the authority) to alter, deface, block, erase, destroy or conceal a record held by the authority if a request has been made for information contained in the record and the applicant is entitled to be given the information.

9. Sections 170 to 173 of the DPA include a number of criminal offences for misusing personal data.

Overview of contents

Section 2 - Records

Definitions

10. For our purposes we define a record as

    - information created, received, and maintained as evidence and information by our organisation or by a member of the Commissioner's staff, in pursuance of our legal obligations or in the transaction of our business
    - information created, received, and maintained as an asset of our organisation in pursuance of our legal obligations or in the transaction of our business

11. This policy covers all records held by the Commissioner and the Commissioner's office irrespective of format or of the technology used to create and store them or the type of information they contain and includes the following:

    - email (including information held in staff email accounts)
    - facsimile (Fax)
    - photographs
    - records in all electronic formats, including discs and CDs, films
    - records in paper format
    - audio files

12. This policy also covers all records in the above formats that have been transferred to the Commissioner by external organisations, for the duration of time that they are held by the Commissioner.

13. The records management system:

    - accommodates paper file systems and records that are created or exist in electronic format
    - provides a simple information structure for logical file storage
    - provides referencing and classification metadata[1] for effective retrieval of accurate and related information

14. Our records must be trustworthy, complete, accessible, legally admissible in court, and robust for as long as our File Plan and Retention Schedule requires. Records that are consistently created, stored correctly and logically indexed are easier to manage to meet these requirements.

[1] The metadata is the set of data that provides information about the record - it provides details of the description and context of the data.

Records Lifecycle

15. The key lifecycle phases of a record are:

Phase 1 – Creation, Receipt, Storage

Records are created or received and (where appropriate) stored in our records management systems

Phase 2 – Maintenance and Use

Records are accessible and being used for the business purpose for which they were created or received

Phase 3 – Review and Retention

Records are reviewed for their value – business, legal, financial, research, historical

Phase 4 – Disposal

Records no longer of organisational value are appropriately disposed of or destroyed beyond any possible reconstruction

16. These phases are described in more detail below.

Phase 1 – Creation, Receipt and Storage

Creation

17. If you create a record (following records creation procedures), it is your responsibility to ensure that the record is filed in an appropriate manner in the correct system.

Receipt

18. If you receive information which should be held as a record in our systems, it is your responsibility to ensure that the record is created following record creation procedures and then filed in an appropriate manner in the correct system.

Record Storage

19. You must save electronic records to the appropriate software package. Section 4 – Software, Network Drives and Roaming Profile provides guidance on this.

20. You must file paper records in accordance with the relevant procedures.

Indexing

21. The File Plan provides a framework for a consistent approach to classifying records across the organisation regardless of format or physical location.

22. The File Plan, in conjunction with the Retention Schedule, is used to identify and retrieve records relating to the same function and activity anywhere in the organisation, irrespective of which department produces or receives them.

23. The File Plan is structured in a three-tier hierarchy representing business functions, activities and sub-activities carried out within the function.

24. You must index all records you create and records you receive from outside the organisation with the applicable system metadata stipulated in the relevant indexing procedures and guidelines in the File Plan

25. The metadata helps us to file, organise and find the records we hold in our records management system.

26. In the context of our records management system and the File Plan the “metadata” includes:

- descriptive metadata – the description of the record
- structural metadata – where the record is held
- administrative metadata – what the record relates to, who can have access to the record

Phase 2 – Maintenance and Use

Maintenance

27. The function-based File Plan and Retention Schedule provides the framework within which the records held by our organisation will be efficiently and effectively managed.

28. Throughout the lifecycle of a record you must ensure that the metadata relating to the record remains current and appropriate and that the record is filed and managed in accordance with the File Plan and Retention Schedule

29. Key Documents must be managed following specific procedures and guidance, as set out in Management and Review of Key Documents Handbook.

Use

30. Records should only be used for the business purpose for which they were created or received.

31. All members of staff are subject to the duties detailed in the:

- IRM Policy
- Employee Handbook (Section 5, para 459 - 470)
- Data Protection Policy and Handbook

Phase 3 – Review and Retention

32. Section 7, together with the File Plan and Retention Schedule and Records Review Procedures, set out the arrangement for managing the review of records.

33. For this process to be effective, it is essential that the processes for Phases 1 and 2 are followed at all times.

Phase 4 – Disposal

34. Once a decision has been made that a record is to be disposed of the correct procedure must be followed to ensure that records are destroyed appropriately

35. Section 7 together with the File Plan and Retention Schedule and Records Review Procedures provides guidance on the correct methods of disposal and destruction of records.

Section 3 - Hardware

Desktop PCs, laptops and mobile phones

36. You are provided with a desktop personal computer (PC), a laptop and a mobile phone.

PCs

37. Your PC will be connected to the Commissioner’s network servers with access to the internet, email, network drives and the necessary software required according to your role.

38. You are responsible for the security and safety of the hardware and any information created and stored on your PC.

Laptops and mobile phones

39. You are also provided with a password protected encrypted laptop and a PIN protected mobile phone to enable you to work remotely. When working remotely you should use your laptop and office mobile phone.

40. You must take all necessary precautions to safeguard the laptop and the mobile phone and the contents of each item. The following must be adhered to:

- if travelling by car, the laptop and mobile phone must be locked in the boot and never left in plain sight
- the laptop and mobile phone must never be left unattended when using public transport or attending an event or meeting
- where a privacy screen and/or a security lock have been issued, these should be used to maintain confidentiality and security for example, when the device is being used on public transport, when the device is being kept in a hotel
- only you may use the laptop and mobile phone
- the laptop and the mobile phone can be connected to an external internet access but this must be a secured network e.g. a home internet which is password protected
- do not connect the laptop or the mobile phone to any external wired/wireless internet access in a public place for example, a café or communal area as the wifi connection is not secure and will be a cyber security risk
- the Employee Handbook (paragraph 889 – 920) sets out the principles under which you are authorised to use the Internet and email systems and these also apply to the use of the internet and email on your laptop and mobile phone
- do not download any software onto the laptop or the mobile phone – if you require specific software discuss this with your line manager and obtain the views of CST – in order to comply with our IT and cyber security policies, all downloaded software needs to be authorised by the FAM before it is downloaded
- each laptop requires a password to access and each mobile phone requires a PIN. Any passwords/PINs given to a member of staff to access a laptop or mobile phone must not be shared with any person. The CST have access to laptop passwords and mobile phone PINs to enable the provision of ICT support.

41. Any theft or loss of a laptop or mobile phone (or any other equipment) must be reported immediately to the HOCS.

42. Cyber security threats, for example, viruses can be introduced into the Commissioner’s network or transmitted to a third party’s system by sending and receiving e-mail, opening attachments and by using the internet. You must take all reasonable steps to ensure that you do not permit or facilitate any cyber security risk and/or threat, including the transmission of any computer virus by you to the Commissioner’s computer systems or to any third-party system.

43. To maintain security the network firewall may prevent access to some websites. If you require access to a blocked site for business reasons email the CST (Admin) with the link to the site and reason that you need access. If it is deemed safe the CST will unblock the site.

44. ‘Zip files’, which usually enter the network as attachments to emails, have a high risk of carrying a computer virus which will activate when the zip file is opened. Of course, some zip files may be legitimate and safe. All emails we receive with zip files attached are automatically marked as ‘SPAM’. Our general policy is not to accept zip files. If you receive an email with a zip file attached either:

- if you know it is SPAM, delete the email and attachment immediately, or.
- if you believe the attachment is genuine, confirm the sender’s identity by calling them (preferred), or by email using an email or telephone number you know is genuine. Advise the sender our policy is not to accept zip files, and ask them to resend the information in unzipped format (e.g. as a series of Word documents). If this is not possible, contact the CST for advice.

Hardware - Other

Memory Sticks

SIC Memory Sticks

45. A number of encrypted are held by CST and available for staff use. CST will ensure that the necessary paperwork is completed before issuing the memory stick.

46. Once signed-out from CST the memory stick and any information contained on it becomes your responsibility.

47. You must ensure that memory sticks remain secure at all times.

48. Any loss or theft of the memory stick should be reported immediately to the HOCS.

49. If you need to take sensitive and/or confidential information out of the office, for example, attending an external meeting, you should, where possible, take this information loaded onto your laptop.

50. In order to access the information contained on an encrypted memory stick the computer being used must have the encryption software installed. The software is available as a free download from the internet and can be installed on any PC/laptop. CST can provide advice and assistance on the use of encrypted memory sticks.

51. Security of the information contained on the memory stick is maintained as it cannot be accessed without the password provided by CST.

Non-SIC Memory Sticks (and other media)

52. We may be sent information on a memory stick or other media, for example, for a presentation or containing withheld information from a public authority.

53. Your PC and laptop are configured to deny access to such devices by default. CST can provide access on a temporary or permanent basis, as appropriate.

Section 4 - Software, Network Drives and Roaming Profile

Introduction

54. The Commissioner provides the necessary software and drives for storing information which have the appropriate access permissions, security and are backed-up. You must use the appropriate software and drives when you create and store records.

Software provided by the Commissioner to manage records

55. The Commissioner uses five key software packages for storing records according to their type. The majority of the Commissioner's records are held within these packages. All PCs and laptops will be pre-loaded with the necessary software depending on your role.

System	Definition
Workpro	Case records related to individual applications for decision, complaints, requests for information, publication scheme approvals, enquiries, and enforcement action
Virtual Cabinet (VC)	Generally, non-case related records of longer term evidential or informational value i.e. which need to be kept for longer than their immediate business use as identified in the Commissioner's File Plan and Retention Schedule
Simply Personnel	Human Resources management software – for HR administration e.g. annual leave and sickness absence
MS Outlook	Incoming and outgoing emails of a transitory nature – these should be deleted once actioned and are no longer of immediate business use – emails that fall within the definition of other system records within this table should be saved to that system
ACT!	Day to day records of communication between the Commissioner and external agencies and individuals that do not form part of cases managed using Workpro

56. If you require additional software for a specific purpose, please discuss this with your line manager. If the purchase/installation of additional software is authorised this can be arranged by CST with the HOCS's approval.

Microsoft Teams (MS Teams)

57. MS Teams – this application includes video and audio call software allowing for virtual meetings and can enable the recording of meetings, a chat function and storage of files, in addition to other collaborative tools within that system. At the present time, the recording of meetings and the chat function have been disabled and staff are not permitted to use these

and other collaborative tools, for example the whiteboard function unless specifically authorised by the HOCS. No case related or sensitive data should be stored using the MS Teams software. Guidance on the use of MS teams has been provide to staff and if you need any further information about how MS Teams can be used you should contact the Administrator.

58. Exceptionally, there may be justification for holding records in a network drive. The following section describes when it is appropriate to do so.

Network Drives

59. All information on network drives forms part of the Commissioner's corporate records and must be managed according to this IRM Handbook and any related guidance or additional guidance provided.

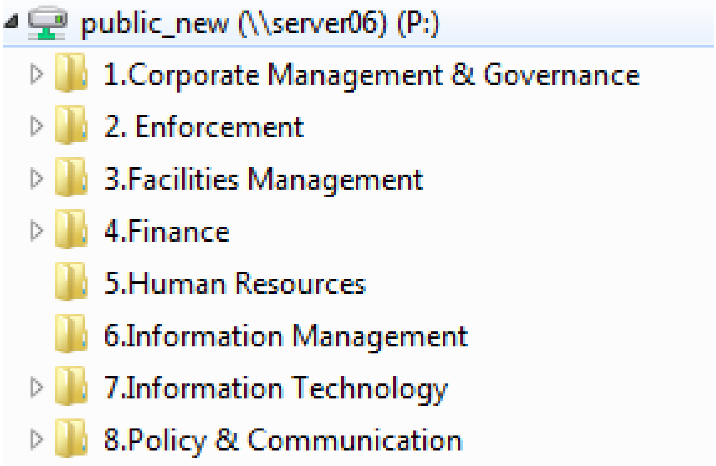
60. You have access to network drives depending on your role, for example, a limited number of staff have access to the S:drive for Sage financial data.

P:drive – Public drive

61. All staff have access to the P: drive. The P:drive is predominantly used for:

- storage for pictures and images used by the Policy and Information Team
- spreadsheets which cannot be linked together in VC
- Workpro templates – master copies for uploading to Workpro
- Scanned documents – Documents scanned on the copier (in the mail room) are automatically saved to P:/XeroxScans/Admin before being re-named and moved as appropriate.

62. The P:drive and its contents are structured and managed to comply with our File Plan and Retention Schedule (see image below) and is part of the daily back-up.



public_new (\\server06) (P:)
1.Corporate Management & Governance
2. Enforcement
3.Facilities Management
4.Finance
5.Human Resources
6.Information Management
7.Information Technology
8.Policy & Communication

63. You must manage all records on the P:drive to comply with the File Plan and Retention Schedule. In particular the contents of XeroxScans/scanning folders should be regularly reviewed and the records moved to the appropriate area.

64. If you have any queries or wish clarification of whether a file should be stored in the P:drive please discuss this with CST.

Z:drive

65. The Commissioner recognises that, exceptionally, there may be occasions when staff wish to have information which does not form part of the Commissioner's corporate records and which it is not appropriate to save within VC or Workpro. For this reason all staff have access to a personal Z:drive.

66. This drive is private to each individual. It can be accessed by the CST as System Administrator, with permission from a HOD. The Z:drive is included in the daily back-ups.

67. There are several risks which arise from storing files in your Z:drive:

- Colleagues may not have access to the necessary up-to-date information should you be off unexpectedly
- Records are not stored appropriately in line with the file plan
- Version control, destruction of records and retention schedule cannot be adhered to
- Records could be inadvertently missed as part of a search in response to an information request.

68. Corporate records, including case records must not be saved to the Z: drive.

69. Draft documents which will become corporate records should be saved to VC to allow version control and colleagues to access the document in your absence. For example, a draft decision must be created from a template within VC rather than saving a draft to your Z:drive (or desktop).

70. Examples of types of information which can be saved to your Z:drive include:

- A document being used for research e.g. a pdf copy of an ICO decision being used as research/reference
- A sample of a document being used for reference e.g. National Archives guidance for preparing an email handbook
- A picture which will be used in a document e.g. pictures used to prepare the copier instructions
- Notes you have made which you will use to assist in delivering a presentation

71. You are responsible for managing the contents of your Z:drive on an ongoing basis to ensure they are kept to a minimum, and that it is being used only when it is not appropriate to save records to ACT!, VC or Workpro. Documents should only be held in your Z:drive temporarily.

S:drive

72. The CST has access to the S:drive where Sage financial records are stored.

73. The S:drive is part of the daily back-up routine.

74. The financial data, in conjunction with the financial paper records held, are regularly reviewed according to the Retention Schedule.

O:drive

75. The O:drive is only visible to staff who have access to ACT! software.

76. The ACT! database file is stored on this drive and is included in the daily back-up routine.

E:drive

77. The SMT and FAM have access to the E:drive

78. The records held on the E:drive are reviewed according to the Retention Schedule.

C:drive

79. You must not save any records to the C:drive on your PC or the laptops. The C:drive does not have access permissions applied and is not backed up.

80. You must use the appropriate software or network drive.

PC and laptop – Desktop

81. Your pc desktop is linked to your roaming profile (see below) and has the shortcuts to the programs you use. The pc desktop should be used only as a temporary area for saving documents prior to moving to the appropriate software e.g. Workpro or VC. It must not be treated as a long-term storage area.

82. For example, it is acceptable to save an email with attachments to your desktop before uploading to Workpro or create a Word document and save it to your desktop before uploading to VC. You must delete it from your desktop once saved to the relevant area.

83. You should ensure that the desktop Recycle Bin on your pc and laptop is emptied on a weekly basis. There is a weekly reminder in your Outlook calendar.

84. There are several risks which arise from storing files on your desktop:

- Colleagues may not have access to the necessary up-to-date information should you be off unexpectedly
- Records are not stored appropriately in line with the file plan
- Version control, destruction of records and retention schedule cannot be adhered to
- Records could be inadvertently missed as part of a search in response to an information request.

85. Corporate records, including case records, must not be stored on your desktop.

86. The files on your pc desktop are backed-up as part of your roaming profile. However, should your profile become corrupt it would be necessary for our IT support company to re-build it and it may not be possible to recover all of the files on your desktop.

87. Your laptop desktop is not backed up so should not be used to save records

Your IT Account (Roaming Profile)

88. Each staff member is provided with an IT account allowing access to the Commissioner’s network. This account is also your “roaming profile”.

89. You are responsible for any action carried out under your IT account. To avoid misuse, you should lock your workstation (on either your pc or laptop) when away from your desk and you must never divulge your pc, laptop password or your security authorisations. You should also ensure that you log out of your account when you are finished. You must never attempt to log on to or use a network account that is not yours.

90. Each time you log on with your username and password to a pc which is connected to the network it will load your roaming profile. This allows you to work at any pc within the office and still have access to your own desktop, emails and documents.

91. When you log on remotely to the office from your laptop with your username and password it will load your roaming profile.

92. Your roaming profile contains the following information:

- Username and password
- Contents of desktop – shortcuts, files and Recycle Bin
- Microsoft Outlook – all email folders and contents
- Contents of My Document
- Contents of My Videos
- Contents of My Pictures
- Contents of My Music
- Contents of Downloads folder.

93. If your emails and desktop are not managed effectively then your roaming profile will be significant in size and will take a long time to load when logging-in.

94. The content of your roaming profile should be cleared as appropriate when you leave the organisation.

Section 5 - Managing Email Messages

Introduction

95. It is your responsibility to manage your email messages in order to ensure that your work can be conducted more effectively. Managing email messages appropriately will also ensure we can comply with the requirements of the DPA, UK GDPR, FOISA and the EIRs.

96. To manage email messages you need to distinguish between email messages that are records of business activities (records), and those that are short-lived or temporary or brief email messages.

97. You must move records from personal mailboxes[2] to ensure they are managed with, and in the same way as, other records.

98. In exceptional circumstances it may be necessary to use personal email accounts for the Commissioner's business. If you have to do this, the following steps must be followed

- you should only use a personal email account with the prior approval of your line manager
- due consideration should be given the confidentiality of the email message and any attachments. Line-management authorisation must be sent to the email address being used, copied to the individual's work account, the line manager's work account and the Head of Corporate Service's (HOCS) work account before any other emails are exchanged. All emails sent to or received by a personal email account must be copied to the individual's and line manager's work accounts. As soon as it is confirmed that the email is held corporately and access on the personal email account is no longer required, the individual must delete them completely from their account and email the line manager and HOCS to confirm this has been done. The HOCS will monitor this to ensure that confirmation of the deletion of emails held on personal accounts is received. Information held in a personal email account will be regarded as information held by the Commissioner and will fall within the scope of requests for information received by the Commissioner. Section 65 of FOISA and regulation 19 of the EIRs apply to this information.

99. Your personal mailbox within Outlook is restricted to a total maximum size of 500MB. Your mailbox should not be used for long-term storage of email messages and should only be used for short-term reference purposes. When these emails are no longer required they must be deleted.

100. You must review your email messages each week to ensure records are identified and moved to the appropriate area, and that those messages which remain in your email folder are only to be used for short-term reference purposes.

101. The Employee Handbook sets out the principles under which you are authorised to use the internet and email systems which you must follow and adhere to (see paragraphs 889 – 920).

[2]. Personal mailbox includes the inbox, where you receive emails which are addressed to you, folders created under the inbox where emails from your inbox might be moved to, and the sent box, where email addressed from you are sent to other people.

Identifying and managing email records.

Essential Principles

102. When an email is sent or received a decision needs to be made about whether the email needs to be captured as a record. Once an email message has been captured as a record it should be deleted from your mailbox.

103. The main points to consider when managing email records are:

- Identifying email records
- Who is responsible for capturing email records
- Email messages with attachments
- When to capture email records
- Where to capture email records
- Subject of email records.

Identification – is the email a record?

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

105. Email messages that might constitute a record are likely to contain information relating to business transactions that have taken or are going to take place, decisions taken in relation to the business transaction, or any discussion that took place in relation to the transaction. (For example, during the decision to publish a tender document for a particular service, background discussion about what this should include might take place via email and should be captured as a record.)

Who is responsible?

106. As email messages can be sent to multiple recipients there are specific guidelines to indicate who is responsible for capturing an email as a record:

RECIPIENT	ACTION
Internal emails	The sender of an email message, or initiator of an email dialogue that forms a string of email messages Exception - as regards Enforcement case files, the Investigations Handbook provides that it is the responsibility of the case owner to save emails in the case file.
Emails sent externally	The sender of the email message
External messages received by one person	The recipient
External messages received by more than one person	The person responsible for the area of work relating to the message

Email Records with Attachments

107. Where an email message has an attachment a decision needs to be made as to whether the message, the attachment, or both, should be kept as a record. The decision on whether an email and/or its attachment constitute a record depends on the context within which they were received. It is likely that in most circumstances the attachment should be captured as a record with the email message as the email message will provide the context within which the attachment was used.

108. There are instances where the email attachment might require further work, in which case it would be acceptable to capture the email message and the attachment together as a record and keep a copy of the attachment in another location to be worked on. In these circumstances the copy attachment that was used for further work will become a separate record.

When and Where to Manage Email Records

109. Email records should be captured as soon as possible.

110. Email messages that constitute records must be saved to the appropriate software -VC or Workpro, ACT! (if applicable).

111. To ensure that the saved email is a true representation and retains the characteristics of the original email it should be saved using the Outlook Message Format (.msg).

112. Most email messages will form part of an email conversation string. Where an email string has formed as part of a discussion it is not necessary to capture each new part of the conversation, i.e. every reply, separately. It may be appropriate to capture email strings as records at significant points during the conversation, rather than waiting until the end of the conversation.

Subject of Email Messages

113. The subject of an email message does not always reflect the reason for capturing a message as a record. This can be avoided through following the guidelines detailed in Section 6 - Records Storage, Version Control, Naming Conventions and Indexing.

114. If the subject of an email does not accurately reflect the reason why it is being captured as a record then it should not be re-named within the mailbox, but at the point it is captured within the software, i.e. the record entry form. Re-naming email records is particularly important when they represent different points in an email string as it will help to identify the relevant aspects of the conversation.

Managing Deleted Items

115. By default, you will be asked to clear your Deleted Items folder when you exit Outlook. You should always say yes to this when you finish for the day. When emails are deleted from your personal Deleted Items folder the email remains in a ‘recover’ folder for 5 days after which it will be automatically deleted by the server. In addition, there can be up to five days backups where there may be a copy of the emails. After the 5+5 days the emails are permanently deleted and cannot be recovered.

116. If you need to access emails in a ‘recover’ folder e.g. for an information request, CST will provide assistance.

117. You must not alter the settings on your PC to retain messages in the deleted items folder.

Good Practice: Making your Mailbox Manageable

118. Managing an email mailbox effectively can appear to be a difficult task, especially if you receive a large volume of email messages regularly. It should not be about following rigid classification guidelines. Instead you find and use a good practice approach that works best for you.

119. There are a number of good practice approaches that might aid the management of email messages. For example:

- Allocating sufficient time each day or week to read through and action email messages
- Setting calendar reminders for the above
- Prioritising which email messages need to be dealt with first
- Looking at the sender and the title to gauge the importance of the message
- Noting where you have been “cc’d‟ into email messages. These messages are often sent ‘for your information’ and do not require immediate/any action
- Setting rules for incoming messages so they can automatically be put into folders
- Using folders to group email messages of a similar nature or subject together so they can be dealt with consecutively
- Identifying email messages that are records or need to be brought to other people’s attention
- Keeping email messages in personal folders only for short-term personal information. Generally, emails that are required for longer purpose should be managed as records
- Deleting email messages that are kept elsewhere as records
- Deleting email messages that are no longer required for reference purposes from the inbox and sent items.

Email management during absence

120. Colleagues may need to access email messages from your mailbox when you are away from the office for an extended period, for example on holiday or because of ill health for example, to respond to an information request or to an enquiry from an applicant, to deal with a business matter

121. The Employee Handbook (paragraphs 889 – 920) set out the principles under which you are authorised to use the Internet and email systems.

122. You must ensure that you give a least one member of your team access to your emails at all times (via Outlook permissions) so that they can be managed during your absence. Line managers, Heads of Department and the FAM should be aware that emails which contain personal data about a member of staff, for example, appraisals, ill health, pay and pension matters may be able to be viewed by another member of staff and, ideally, the content of such email correspondence should be managed using VC instead, for example, it may be fine to send an email requesting a return to work meeting but the content of the meeting and the note of the meeting should be stored in the staff member's folder in VC.

123. If you have not delegated access, or the delegated staff member is not available, authorisation to access the email system should be sought from the appropriate Head of Department (HOD).

124. If access is authorised the HOD should advise CST and access will be arranged.

Management of Shared Mailboxes and Public Folders within Outlook

Shared Mailboxes (with unique assigned email address)

125. Shared mailboxes should be used where there are a group of people responsible for the same area of work. Using a shared mailbox can be a way of ensuring that queries are answered quickly when members of the team are away from the office. Access to a shared mailbox is initially given by approval from the SMT and will be actioned by CST.

126. There are a number of shared mailboxes currently in use e.g. enquiries@itspublicknowledge; sic@itspublicknowledge.info and media@itspublicknowledge.info.

127. It is the responsibility of the identified owner to establish procedures for the management of the shared mailbox, and to communicate them to the other members of staff who have access to it.

Public Folders (for short term storage of emails received by any mailbox)

128. There are a small number of public folders set up on the network server with access determined by the owner and function of the folder. For example, a public folder would be set up to store responses to an invitation to an event or responses to an invitation to tender.

129. A public folder is for short term use only and the records contained within the folder will be reviewed in accordance with the File Plan and Retention Schedule.

130. When managing public folders, the owner of the folder should provide clear rules as to how the folder will be managed. This should include all the points detailed in the Identifying and managing email records section. These rules need to be recorded and filed in VC and need to be notified to CST.

131. The owner of the folder must ensure that the messages remain in the folder no longer than the pre-agreed time period. After this time, messages should either be deleted or managed as records. It is also the responsibility of the folder owner to delete the folder once it is no longer required.

Levels of Responsibility – Shared Mailboxes and Public Folders

132. Although the purpose of shared mailboxes and public folders is different there are some similarities in the way in which they should be organised. If a shared mailbox or a public folder is going to be used the following areas must be addressed so that the email messages contained do not become unmanageable and appropriate records are identified:

- identifying an owner
- the purpose
- access
- managing the contents of shared mailboxes and public folders.

133. Identifying an owner - When a shared mailbox or a public folder is created one person must be identified who can take ownership of the folder or mailbox. For shared mailboxes the owner should be responsible for developing rules governing how email messages are responded to and how this is communicated to other people.

134. The CST has administrative responsibility for maintaining shared mailboxes and public folders. If the owner has any specific problems with managing the shared mailbox or public folder these should be discussed with their HOD.

135. The purpose – The creation of a shared mailbox or a public folder should be done with a specific purpose, for example a public folder might be created to allow replies to a conference invitation to be stored until the event is passed. It is the responsibility of the owner of the shared mailbox or the public folder to ensure that the mailbox or public folder is used for the specified purpose. If the shared mailbox or public folder is not being used for the specified purpose the owner should discuss this with their HOD and notify CST

136. Access – The level of access granted for shared mailboxes and public folders is likely to be different. For shared mailboxes access will only be granted to people who are able to answer the emails that will be received. In shared mailboxes it might also be necessary for the owner to delegate some responsibility to other people who will be granted access in terms of managing the emails and ensuring the mailbox is used for its specified purpose.

137. Managing the contents of shared mailboxes and public folders - In the case of shared mailboxes, management is to be shared between everyone who has access. In the case of public folders management, the folder owner is responsible.

138. The default access to a public folder is that a member of the CST or a HOD can view the contents of a folder.

Section 6 – Records Storage, Version Control, Naming Conventions and Indexing

Introduction

139. The efficient location and retrieval of information is vital to support the effective running of the organisation and to comply with the requirements of the DPA, UK GDPR, FOISA and the EIRs.

140. This is achieved through the consistent and rigorous application of naming conventions, the application of version control guidance and by following indexing and storage guidance.

Section Contents

141. Guidance relating to this area of records management is laid out as follows:

- Record Storage – Paper
- Record Storage – Electronic
- Version control guidance
- Guidance for naming conventions, indexing and filing documents and folders

(a) VC

(b) Workpro

(c) ACT!

Record storage areas - Paper

142. Filing Cupboards– placed in staff offices and used for hard copies of case related documentation (i.e. original paper records and other 'hard' format records (e.g. memory stick's)) only where absolutely required. Documentation is contained in folders labelled with basic Workpro information about the case (Workpro number, Applicant name and Authority name). The cupboards must be kept locked at all times, except when in use.

143. Secure Store – used for storage of confidential documents and governance and finance records required for the operation of the Commissioner's business, e.g. highly confidential information submitted by an authority in the course of an investigation, prior years invoices and accounts information. These records should be registered either in Workpro (if they relate to an investigation) indicating where they are located (i.e. in the Secure Store), or in VC (if they are required for the operation of the Commissioner's business), again, indicating where they are located. This store must be kept locked at all times, except when in use. The Secure Store must not be used for storage of any non-case related records containing personal data e.g. recruitment documentation or HR files, nor should it be used to store tender submission documents prior to the tender opening date.

144. 'Bell' – where absolutely required, the CST create and hold some records in paper format to fulfil the operational functions of the Commissioner, such as hard copy personnel files or recruitment records. Files for such records must be registered in VC. These are held in locked cupboards or filing cabinets in Bell and Elliot. In the case of hard copy HR and

recruitment files, the keys to the filing cabinets where these documents are stored are held by the HOCS and the FAM only.

145. Other Locations – Lockable cupboards and desks may be used to store non-case related documentation e.g. working papers, project files. You are responsible for managing these paper records on an ongoing basis to ensure they are kept to a minimum, and that they are being used only when it is not appropriate to save records in the locations detailed above.

Register of paper records

146. A register for non-investigation paper records is maintained at VC21798. The Register is updated regularly and provides guidance on where to store and/or locate paper records.

Record Storage areas- Electronic

147. The Commissioner provides you with the necessary software to allow you to create, manage and retrieve records. Section 4 – Software, Network Drives and Roaming Profile provides further guidance.

148. You should use the appropriate software according to the function of the record and ensure that records of a similar nature are stored together.

Version Control Guidance

VC

149. All records stored in VC are subject to version control. Versions are created when a new record is established, and subsequently each time the record is ‘checked in’. This feature supports good management of general records by enabling users to review and manage previous versions of records and provides an audit log of all activity for the record. Further guidance is provided in the VC User Manual which is accessed by clicking the ? in the top right corner of VC.

150. Specific arrangements apply to the use of version control in the management of key documents which must include a Document Control Sheet. The Key Documents Handbook details the policy, procedures and guidance to be followed in the creation, approval and review of key documents, as set out in the associated Register of Key Documents.

Workpro

151. Workpro uses Microsoft SharePoint to manage records held within individual electronic case files. SharePoint creates a new version of a record each time it is edited and closed and all versions are stored in the SharePoint database. The Workpro document user interface does not display information relating to version control.

ACT!

152. Records stored within ACT! can be edited, but version control is not available. An audit trail is available which records the date and time when records are uploaded to ACT!.

Network Drives

153. A limitation of holding records in network drives is that they do not benefit from version control. These records do have basic metadata which provides an audit trail of creation and the last review of the record.

Virtual Cabinet - Guidance for indexing and filing documents and folders

Using Interests, Subjects and Document Types

154. Each cabinet in VC has a set of mandatory index fields that must be completed when indexing a document in VC for the first time, either when creating a document or when moving an existing document into VC. These are:

- Description – meaningful description of record, including naming convention where appropriate
- Document Author – the staff member creating new records or capturing records from external source
- Organisation – most likely to be 'OSIC', specific body or supplier; where you think an organisation is missing please index it against the "missing organisation" value. (see paragraph 156)
- Subject – the subject related to the document you are creating. Where you think a subject is missing please index it against the "missing subject" field value. (see paragraph 156)
- Document Types - refer to the format or layout of the documents being filed.

What if I have problems indexing a record in VC?

155. Check the appropriate section of File Plan and Retention Schedule for guidance.

156. If you still feel there is no appropriate index value for the record, index the record against "Missing Organisation" in the Organisation Index Field or "Missing Subject" in the Subject Index Field. This will enable you to index the record without having to wait for the change to be actioned. Please advise CST of the required update to the organisation or subject. Once CST confirm the change has been made you can reindex the original document.

VC– Guidance on Naming Conventions

157. Take the time to provide a concise and reliable description for the record and assign it to the most relevant interest, subject and document type that applies to it in VC (see the File Plan and Retention Schedule for help with this).

158. Presume a future searcher has no prior knowledge about the record you are naming or describing, e.g. a procedure document about naming documents in VC, could be named "Naming documents in Virtual Cabinet"; it should not be named "File classification in the records management system", even though this may mean the same thing to you. The chances are that a future searcher looking for guidance on naming documents will not even think of using a search involving the words "file" or "classification scheme".

159. You should keep descriptions relevant to the record. Do not use redundant words or information like 'general' or 'miscellaneous' or 'N/A'.

160. In general, don't duplicate information. If you discover that a word in your description will appear in an index field, then leave it out, e.g. "Procedure for creating documents in VC" should become "Creating documents in VC" and its document type will be marked as a "Procedure".

161. You should make titles/descriptions concise – simple, short and meaningful. There should be no long document descriptions.

162. You should create titles/descriptions that are static and do not require to be changed regularly, e.g. issue numbers for handbook documents. If an element needs to be changed regularly, it can be shown elsewhere, either in the index fields or in the document itself.

163. Do not use abbreviations or numbers, or meaningless classification schemes in the description field – e.g. Budget SIC 2019-20 Original CE which would mean nothing to a newcomer to the organisation.

164. Dates - Where the date is required in a document description e.g. meeting records, contracts etc. it should be at the beginning of the description. This enables a chronological listing of the records in the search results window and it is easy to spot any missing records in a series. Dates should be in the following format:-

- Full date - YYYY MM DD e.g. 2019 09 26
- Month – YYYY MM e.g. 2019 09
- Year – YYYY e.g. 2019
- Range of years – YYYY – YY e.g. 2019 – 20

165. Organisation names - The organisation name should match the formal name used by the organisation – e.g. in letter heading.

166. Which system “owns” the master organisation list?

- Scottish Public Authorities – Workpro
- Commissioner’s Suppliers – SAGE

167. The following table provides naming convention guidance for records created for activities common across the organisation. This table will be added to over time as naming conventions are agreed within the organisation.

VC – Cross function records

Filing Location/Activity	Record type	Convention	Notes/keyword selection
Cross function			
	Meeting Minutes	YYYY MM DD [Meeting name] Minute e.g. 2019 11 03 QSMTM Minute	Where it is a regular meeting, the abbreviated Meeting name should be used as the record will be indexed against the full meeting name under subject. Where the meeting is ad hoc, a brief meaningful description of the meeting should be used.
	Meeting Agenda	YYYY MM DD [Meeting name] Agenda e.g. 2019 11 03 QSMTM Agenda	

VC –Individual Functions

168. The following table provides naming convention guidance for records created for activities carried out by individual functions. This table will be added to over time as naming conventions are agreed within the organisation.

Filing Location/Activity	Record type	Convention	Notes/keyword selection
Corporate Management and Governance			
		YYYY MM DD [meaningful description]	
Enforcement			
Investigation	Draft Decision Notice	Draft Decision John Smith and Scottish Ministers 202000161	
Investigation	Final Decision Notice	YYYY MM DD Decision 123/2013 John Smith and Scottish Ministers 202000161	Should be created from the final version of the draft and should only have 1 version. Date is the date of issue.
Investigation	Anonymised Decision Notice for publication	YYYY MM DD Decision 123/2013 ANON Applicant and Scottish Ministers 202000161	Should be created from the issued version of the decision notice and should only have 1 version. Date is the date of issue.
Quality Assurance	Completed forms	YYYY MM DD [Name of Assessor/Officer] [Name of form] [WP reference] e.g. 2019 10 01 EM/GW QA Records Management 201900099	The date represents the date of sign off of the form by the Assessor
Facilities Management			
		YYYY MM DD [meaningful description]	
Finance			
Insurance	Policies, Schedules, Certificates	YYYY MM DD – YYYY MM DD [insurance subject] [record type] e.g. 2019 06 01 to 2020 05 31 Buildings insurance policy	The dates represent the start and end dates of the policy. Use the Organisation field for the external company name.
Payroll &	Expense claims	YYYY MM Expenses Claim	

Filing Location/Activity	Record type	Convention	Notes/keyword selection
Expenses		[staff initials] e.g. 2019 08 Expenses Claim JS	
Procurement/Contract Management	Contracts	YYYY MM DD to YYYY MM DD [subject of contract] contract e.g. 2019 06 01 – 2020 05 31 Health and Safety contract	The dates represent the start and end dates of the contract. Use the Organisation field for the external company name.
HR – (staff name) Admin		YYYY MM DD [meaningful description]	
HR – (staff name) Personal			
Performance & Development Framework	Form A – Forward Work Plan	YYYY - YYYY [Line Manager/Staff initials] Forward Work Plan	
	Form B – In-Year Review Meeting Record	YYYY MM DD [Line Manager/Staff initials] In-Year Review Meeting Record	Where the date is the date of the meeting.
	Form C – Review Self-Assessment	YYYY to YYYY [Staff initials] Annual Review Self-Assessment	
	Form D - Review Meeting Record	YYYY MM DD [Line Manager/Staff initials] Annual Review Meeting	Where the date is the date of the meeting.
Human Resources			
		YYYY Timesheet [staff name] 2019 Timesheet J Smith	
Information Management			
		YYYY MM DD [meaningful description]	
Information Technology			
		YYYY MM DD [meaningful description]	
Policy and Communication			
Publications and Guidance	Open Update newsletter	[month] Open Update e.g. February 2021 Open	Month is the month of issue of the newsletter

Filing Location/Activity	Record type	Convention	Notes/keyword selection
		Update	

Workpro - Guidance for indexing and filing documents and folders

169. It is good practice to apply consistent naming conventions across all records regardless of where the records are created and stored. The naming rules for Workpro are similar to those for VC documents, i.e. keep the name as clear, concise and informative as possible. It should identify the format (e.g. letter, e-mail), either who the document is to (if outgoing), or from (if incoming), and a brief note on what it is about e.g. "Year/Month/Date E-mail from Scottish Government explaining new request handling procedures".

170. The Investigations Handbook contains records management guidance on naming documents in Workpro.

171. When sending emails to Workpro consider including the case number in the title of the email. This will make it much easier when attaching the email to the case within Workpro.

ACT! - Guidance for indexing and filing documents and folders

ACT! – Guidance on Naming Conventions

172. When naming records saved within ACT! you should ensure that:

- Date is in the format YYYY MM DD at the start of the description
- Titles are concise and meaningful

173. If saving several emails regarding the same topic either:

- save the final email with the full string of the conversation, appropriately renamed; or
- save at significant point throughout the conversation amending the title to reflect the agreed point/decision.

Section 7 – Review and Disposal of Records

Review of Records

174. Phase 3 in the Records Lifecycle relates to the review and retention of records.

175. There are consistent and documented retention, selection and disposal procedures for deciding and managing the various categories of records held by the SIC.

176. The IRM Policy requires that the Commissioner's records are:-

"….regularly reviewed to maintain the integrity of the retention guidance. Implementation of this guidance will:

177. Regularly reviewing records, ensuring that requirements of the File Plan and Retention Schedule are met, will enable us to:

- conduct the Commissioner's business properly
- maintain a suitable and precise corporate memory
- develop a knowledge base of skills and experience.
- support the Commissioner's IRM Policy by providing appropriate guidance for authoritative and auditable disposal decisions and actions.
- assist in identifying records that may be worth preserving permanently as part of the Commissioner's archives.
- prevent the premature destruction of records that need to be retained for a specified period to satisfy legal, financial and other requirements of public administration.
- provide consistency for the destruction of those records not required permanently after specified periods.
- avoid the costs and potential liabilities of retaining information the Commissioner does not need and may lead to non-compliance with the FOISA, the EIRs, the DPA and the UK GDPR and, also, possible legal action against the organisation.
- ensure accurate indexing of records.

178. In order to comply with the requirements of the IRM Policy, a review of all records held should be carried out on an annual basis for each function.

Review Planning

179. The reviews are staggered throughout each year.

180. Each team within the organisation (Corporate Services Team, Enforcement and Policy & Information) is assigned a three month period (quarter) within each year to lead the review of all records held across the organisation for that function, both electronic and paper.

TEAM	Annual Review Schedule
Policy & Information	
Policy and Communication	Quarter 1 (April – June)
Enforcement	
Enforcement	Quarter 2 (July – September)
Corporate Services Team	
Corporate Management and Governance	Quarter 3 (October – December)
Facilities Management	
Finance	
Information Management	
Information Technology	
Human Resources	
ACT! records	Quarter 4 (January – March)

181. Heads of Department should refer to the Records Review Procedures for guidance in carrying out a review of records within their team and should ensure that the records review is carried out.

182. Documentation which supports the information and records management process is reviewed annually in Quarter 4 by the HOCS.

Information and Records Management Policies and Procedures – Review Schedule	
Name	**Schedule**
Information and Records Management Policy	Quarter 4 (January – March)
Data Protection Policy and Handbook	
Information and Records Management Handbook	
File Plan and Retention Schedule	
Record Review Procedures	

Disposal of Records

183. Phase 4 of the Records Lifecycle relates to the disposal of records, which occurs following completion of the review process.

184. Disposal of records is an important part of records management and ensures that the organisation retains records only for as long as they are needed and then disposes of them in an appropriate manner.

Disposal of Electronic Records

185. The Records Review Procedures provide guidance on how and when electronic records are deleted.

Disposal of Paper Records

186. The Commissioner operates a ‘shred all’ policy and has in place a contract to carry out the secure onsite destruction of all waste paper.

187. There are a number of secure locked consoles throughout the office which you must use to dispose of all paper waste. The only exceptions are magazines and periodicals which should be put directly into the blue recycling bin. Failure to follow this procedure may be considered a breach of security, in which case the disciplinary procedures set out in the Employee Handbook will apply.

188. Section 34 of the Environmental Protection Act 1990, as detailed in the Code of Practice[3] requires organisations/person which are subject to the Duty of Care to keep records of the waste they receive and consign using a Waste Transfer Note. The Commissioner maintains a Waste Transfer Note which is renewed annually.

[3] http://archive.defra.gov.uk/environment/waste/controls/documents/waste-man-duty-code.pdf

Section 8 - Disposal of IT Equipment

189. Obsolete IT assets, for example, PCs, servers, laptops and hard discs, are generally disposed of due to obsolescence rather than being disposed of as being surplus to requirement. An obsolete IT asset should not be offered for sale and must be disposed of securely to ensure the security of any data that may still be held on the IT equipment is not compromised.

190. A fixed asset disposal approval form (Appendix A of the Finance Policy - Fixed Assets) must be completed for each piece of equipment and must be signed by the HOCS, giving approval to dispose of the equipment.

Actions prior to disposal

191. The following actions must be undertaken before any piece of IT Equipment is disposed of:

- all fields in the fixed asset disposal approval form should be completed and a copy of the original invoice should be attached to the form
- the fixed asset disposal form should set out clearly what will happen to the IT equipment that is being disposed of.
- If the IT equipment contains a hard disk, the hard disk should be wiped clean using software recommended by the Commissioner's external IT service provider (instructions are in the IT & Telephone Manual) or wiped clean by the Commissioner's external IT service provider contract disposal service providers to arrange secure disposal of the IT equipment. Obtain quotes from at least 2 providers, asking for details of the following:
    - Security accreditation
    - Security and tracking on vans
    - Staff screening
    - Their own security audit process
    - Compliance with WEEE Regulations 2013
    - What happens to hard drives – possible to shred hard drives at OSIC?
    - What happens to other parts of the pc/server/laptop - destroyed/recycled/reused?
    - Confirmation that Certificates of Destruction will be provided for each individual piece of equipment.
- before any IT assets are disposed of a signed contract must be in place to ensure that:
    - there is an appropriate level of security in place (Para 15 of the Data Protection Policy)
    - explicit directions on the services to be undertaken are given
    - adequate data protection measures are taken - a specialist service provider for the disposal of IT equipment may be considered to be a "data processor" under the DPA if the IT equipment contains personal data. If so, you need to ensure that there are adequate contract terms in place to cover the processing that will take place.

Disposal of equipment

192. The following actions should be undertaken when the IT Equipment is disposed of:

- where possible, hard drives should be shredded at the office premises
- if any IT equipment needs to be taken away from the office premises for disposal, a list of equipment to be taken off site by the service provider should be prepared and the service provider should sign the list to confirm what equipment they are removing.
- the service provider should provide a Certificate of Destruction for all of the IT equipment being disposed of, including the component parts of equipment, showing serial numbers and the method of destruction.
- all Certificates of Destruction must be scanned and filed in VC and hard copy kept with the Fixed Asset Disposal Form in the Fixed Asset Folder in Bell.
- if, despite the security measures taken above, a pc, laptop or server is lost by the service provider the HOCS will take the following actions:
    - assess the risks associated with the breach, and
    - if the IT equipment holds any personal data, arrange for a Data Incident Management Plan to be prepared
    - inform the appropriate people and organisations that the breach has occurred
    - investigate the cause of the breach and evaluate the effectiveness of our response and, if necessary, update the Commissioner’s procedures accordingly.

Section 9 – Competences Framework

Role:
Head of Corporate Services

Function:
Information and Records Management

Summary Description:
Overall responsibility for information and records management (IRM) function.

Responsibilities:

- Responsible for IRM related policies and procedures
- Maintains the procedures which support IRM Policies
- Liaises with IRM support staff, the Commissioner and Heads of Departments
- Monitors levels of compliance with the IRM Policies and relevant procedures and guidance
- Communicates IRM Policies and Procedures, and any changes, to all members of staff
- Ensures the provision of information management training for all staff, as required
- Ensures information management policy and relevant procedures are included in all induction courses
- Ensures requirements relating to legislation and regulations, are incorporated into IRM Policy and Procedures, as appropriate and as required
- Identifies requirements for new, or new versions, of IRM software applications
- Ensures IRM implications and requirements are assessed as part of the planning process of new initiatives

Required Core Skills & Training Methods:

Core Skill	Attainment Method
Understanding of basic IRM concepts and requirements	External training
Understanding of the different IRM systems within SIC and can explain them to others – VC, WP, ACT!, Outlook etc..	Review of current practice and past experience and performance; on-job training; use of support manuals
Is familiar with the Commissioner's IRM Policies, Procedures and Processes and can explain them to others	Drafting of policies and procedures Providing internal training
Effectively and efficiently handles colleagues' information management and system enquiries, with the assistance of IRM support staff where required	Review of current practice and past experience and performance; use of support manuals
Is able to carry out IRM system and practice performance monitoring, review and reporting activities	Use of appropriate audit and management tools

Role:
Finance and Administration Manager/Administrator

Function:
Information and Records Management Support

Summary Description:
Providing operational support for IRM function

Responsibilities:

- Administration of the different IRM systems within the Commissioner's office
- Assist staff in activities supporting implementation of File Plan and Retention Schedule including file clear-ups and re-indexing of records
- Supporting IRM system and practice performance monitoring, review and reporting activities
  - actively reviewing records and files to ensure they are correctly named, indexed and stored and maintained
  - carrying out periodic checks to ensure long term preservation of records to ensure they can continue to be retrieved and accessed
- Providing first-line support for staff in relation to IRM systems, processes and procedures, with support of external third parties where required
- Monitor review and disposal activities, and assist the Heads of Department with carrying out timely destruction of expired documents and records
- Provide induction training in IRM policies, procedures and systems
- Maintain registers of non-investigation paper records, as required
- Implement security requirements and access rights to documents and records

Required Core Skills & Training Methods

Core Skill	**Attainment Method**
Understanding of basic IRM concepts and requirements	External training
Understanding of the different IRM systems within the Commissioner's and can explain them to others and can carry out system admin tasks	Review of current practice and past experience and performance; on-job training; use of support manuals
Is familiar with the Commissioner's IRM Policies, Procedures and Processes and can explain them to others	Drafting of policies and procedures Providing internal training
Effectively and efficiently handles information management and system enquiries from staff, with support of external third parties where required	Review of current practice and past experience and performance; use of support manuals
Is able to carry out basic IRM system and practice performance monitoring, review and reporting activities	On-job training and use of support manuals

Role:
Senior Management Team

Function: Head of Department

Summary Description:
Support organisational approach to IRM activities within their team in line with the Commissioner's IRM policies, procedures and systems and ensure that these continue to meet the needs of their team over time

Responsibilities:

- Facilitation role between the Commissioner's teams and the HOCS
  - Communicate to the HOCS and the FAM/Administrator progress, decisions and required actions related to IRM function within their team
  - Feedback information management issues raised by their team to the HOCS
- Leads/co-ordinates one-off and regular IRM activities within their team e.g. file clearing, identification of vital records
- Encourages a high standard of compliance with IRM policies and associated procedures within their team
- Participates in development, implementation, maintenance and review processes in relation to aspects of information and records management required by their team e.g. sections of File Plan and Retention Schedule

Required Skills and Training Methods

Core Skill	**Training Method**
Understanding of basic IRM concepts and requirements within the context of their area of work	In-house training
Understanding of the different IRM systems used by their team and can explain them to others – VC, WP, ACT!, Outlook etc..	Review of current practice and past experience and performance; on-job training; use of support manuals
Is familiar with the Commissioner's IRM Policies, Procedures and Processes and can explain them to others	In-house training

Role:
All Staff

Function:
Records custodians

Summary Description:
It is the responsibility of all staff to ensure that they keep appropriate records of their work in the Commissioner's office and manage those records in keeping with the IRM policy and associated procedures and guidance

Responsibilities:

- Understands and complies with IRM policies and procedures
- Creates records and information that adequately documents the decisions and processes they undertake as part of their duties
- Captures information in the correct records system and has awareness of good filing practices so that information can be quickly retrieved
- Finds needed information effectively and efficiently
- Carries out destruction of paper and electronic information, which is of no significant operational, informational or evidential value requiring its retention, as soon as that information has served its purpose.

Required Core Skills & Training Methods:

Core Skill	**Training Method**
Understands basic IRM concepts and requirements	Induction training
Understands o different IRM systems within the Commissioner's office – VC, WP, ACT!, Outlook etc..	Induction training; review of current practice and past experience and performance; on-job training; use of support manuals
Is familiar with the Commissioner's IRM Policies, Procedures and Processes	Induction and in-house training

Section 10 – Compliance Monitoring

Compliance Monitoring

193. The following table details how the HOCS will monitor compliance with our records management procedures:

	Document title	Compliance Check	Review Frequency
1	IRM Policy	Review of compliance with legislation Update to ensure it reflects current practice & procedures in the Commissioner's office	Per Register of Key Documents
2	IRM Records Management Plan	Review of compliance with legislation and guidance Update to ensure it reflects current practice & procedures in the Commissioner's office	Per Register of Key Documents
3	Information and Records Management Handbook	Review of paper records storage arrangements Review of paper records destruction arrangements Review of paper and IT destruction arrangements Review of compliance with security arrangements (IT and paper)	Three years
4	File Plan & Retention Schedule	Review retention periods for records containing personal data	Two Years
5	Key Document Handbook		Three years
6	Records Review procedures		Annual
7	Annual assurance report to Commissioner/SMT		Annual

194. The review frequencies are determined taking a risk-based approach, and will be revised in light of experience.

Related policies and guidance – relevant to records management

195. The following policies and procedures also contain guidance on the handling of information and are relevant to and are taken account of in our records management procedures.

Data protection

196. The Data Protection Policy and Handbook sets how we comply with the requirements of the Data Protection Act 2018 (DPA) and the UK GDPR and provides guidance to all staff on the following:

- Processing of personal data

- Individual rights
- Accountability
- Data protection by design and default
- Data protection impact assessments
- Data Protection Officer
- Security of information
- Breaches of personal data and data incidents
- International transfer of personal data
- Governance arrangements

197. This key document also contains advice and guidance on the management of subject access requests made to the Commissioner

198. The HOCS is the Responsible Manager for this key document and will carry out a review on an annual basis and, also, as required during any year.

Employee Handbook

199. The Employee Handbook sets out the policies and procedures that will apply to a member of staff during their employment with the Commissioner.

200. The HOCS is the Responsible Manager for this key document and will carry out a review on an annual basis and, also, as required during any year.

Responding to Information Requests and Procedures (Commissioner's internal procedures)

- This key document sets out the internal procedures that should be followed by the Scottish Information Commissioner (Commissioner) and their staff on receipt of, and in responding to requests for information or review under:
  - i. the Freedom of Information (Scotland) Act 2002 (FOISA) and
  - ii. the Environmental Information (Scotland) Regulations 2004 (the EIRs)
- The HOCS is the Responsible Manager for this key document which is currently under review by an internal working party led by the HOE.

Investigations Handbook

201. The Investigations Handbook sets out the procedures for investigations under FOISA, the EIRs and the INSPIRE (Scotland) Regulations and also contains advice and guidance on:

202. The HOE is the Responsible Manager for this key document and will carry out a review every 5 years, or as required within the review period.

Document control sheet

Document Information	
Full name of current version: Class, Title, Version No and Status. *E.g. C5 Key Documents Handbook v01 CURRENT ISSUE*	C5 Information and Records Management Handbook v04 CURRENT ISSUE
VC FileId	153684
Type	Procedure
Approver	SMT
Responsible Manager	HOCS
Date of next planned review	07/2024
Approval & Publication	
Approval Date (major version)	30/06/21
For publication *(Y/N)*	Y
Date published	30/06/2021
Name of document in website file library	InformationandRecordsManagementHandbook
Corrections / Unplanned or Ad hoc reviews (see Summary of changes below for details)	
Date of last update	

Summary of changes to document				
Date	**Action by** *(initials)*	**Version updated** *(e.g. v01.25-36)*	**New version number** *(e.g. v01.27, or 02.03)*	**Brief description** *(e.g. updated paras 1-8, updated HOPI to HOCS, reviewed whole section on PI test, whole document updated, corrected typos, reformatted to new branding)*
30/06/21	BOW	04.00	04.01	New document created following approval of draft
30/06/21	BOW	04.01	04.02	DCS updated, published on website

Scottish Information Commissioner
Kinburn Castle
Doubledykes Road
St Andrews, Fife
KY16 9DS

t   01334 464610
f 01334 464611
enquiries@itspublicknowledge.info

www.itspublicknowledge.info