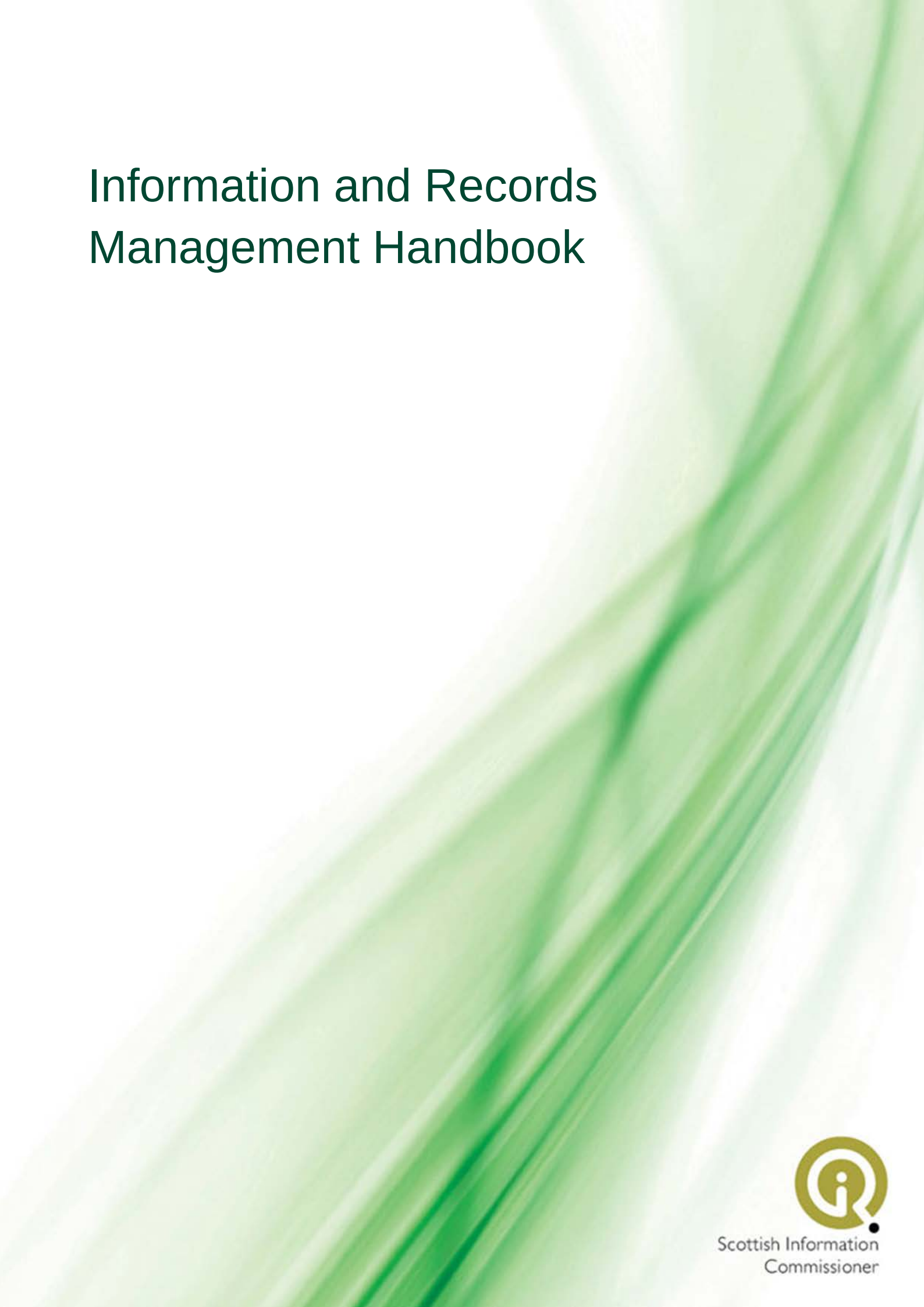
Information and Records Management Handbook



Contents

Glossary and abbreviations

Term used	Explanation
EIRS	Environmental Information (Scotland) Regulations 2004
FOISA	Freedom of Information (Scotland) Act 2002
SIC, the Commissioner	The Scottish Information Commissioner, staff of SIC (depends on context)
DPA	Data Protection Act 1998
HOCS	Head of Corporate Services
HOE	Head of Enforcement
HOPI	Head of Policy & Information
HOD	Head of Department
CST	Corporate Services Team
Systems	The term 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 CS allowing a staff member access to the SIC computer systems (as detailed above)
Ephemeral	Short-lived, temporary, brief

Section 1 – Introduction, Scope and Responsibilities

Introduction

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

2. The key purpose of this handbook is to ensure that you:

   (i) are aware of the controls in place to manage and maintain security of systems, and apply them consistently

   (ii) you are aware of SIC's procedures and guidance for information and records management, and apply them consistently.

Scope

3. This handbook applies to:

   (i) all SIC staff including permanent, temporary and fixed term employees during the course of their employment with SIC

   (ii) all contractors and agents who, at any time, use or may have access to the SIC's internet, email and other business communications systems during the course of their business with SIC

   (iii) any other person authorised to access the SIC business systems.

Responsibilities

4. It is your responsibility to comply with this handbook. You must therefore ensure that you are familiar with its contents and the contents of any associated guidance as detailed.

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

6. 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.

Overview of contents

Section:		Provides procedures and guidance on:
2	Records	The definition of a record The record lifecyle
3	Hardware	Your responsibilities for the security and safety of: • your desktop PC • SIC laptops • memory sticks and any information stored on them
4	Software, Network Drives and Roaming Profile	Where you should (and should not) store information and records: • Software Packages o ACT! o Workpro o IVC o MS Outlook • Network drives o E, P, S, Z drives • PC drives o C drive o Desktop o Explanation of 'Roaming Profile'
5	Managing Email Messages	Your responsibilities for managing email messages: • identifying emails which are records • when and where to save email records • deleted items Good practice guide to help you make your mailbox manageable Email management during absence Management of shared mailboxes and public folders
6	Records Storage, Version Control, Naming Conventions and Indexing	How to correctly name, index and store records: • Storage areas in SIC: o electronic o paper • Storage procedures for paper records • Handling guidelines for paper records • Version control guidance • Guidance for naming conventions, indexing and filing documents and folders
7	Review and Disposal of Records	Guidance on the importance of reviewing records incorporating a records review annual planner. Guidance on the appropriate disposal methods available.: • Disposal of Records: o electronic o paper • Disposal of IT equipment
8	Disposal of IT Equipment	Guidance on the disposal of IT equipment
9	Competences Framework	The competences relating to Information and Records Management roles and responsibilities

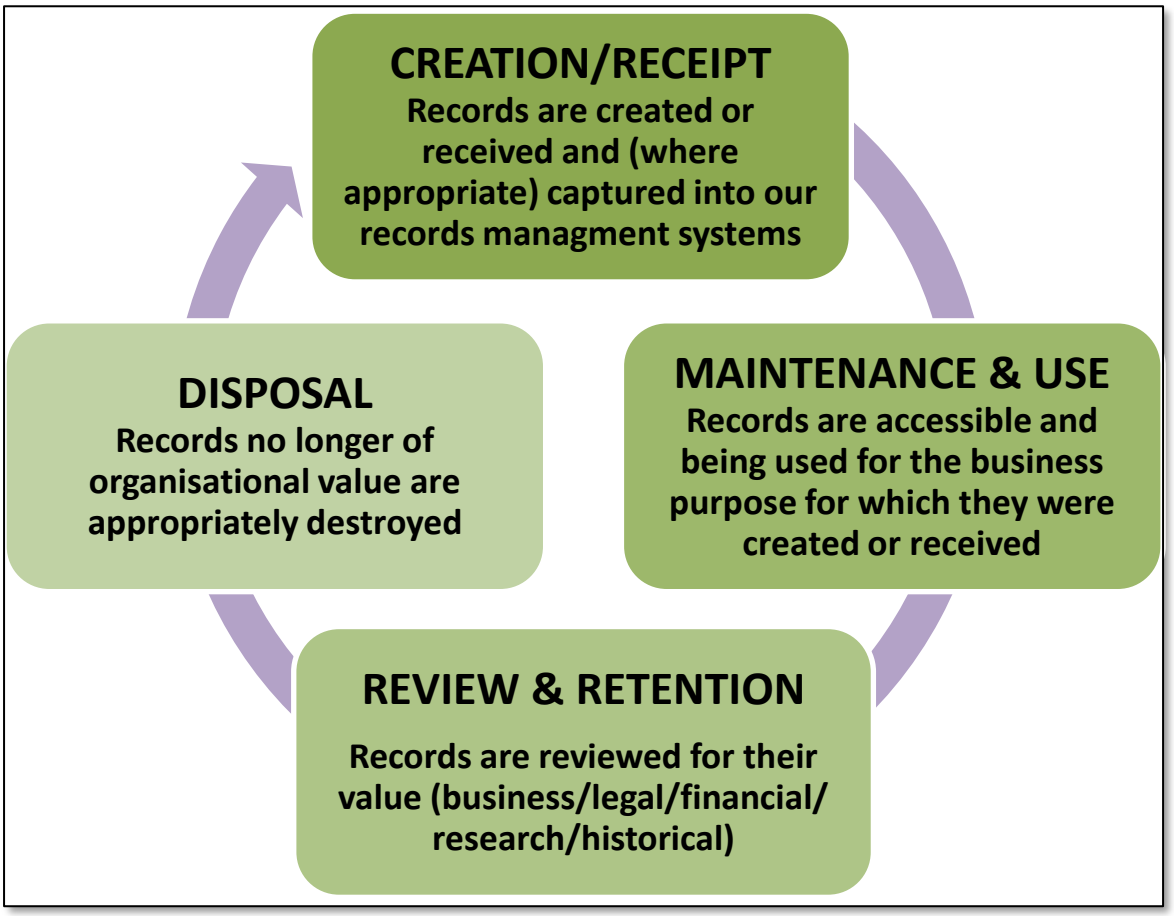
Section 2 - Records

Definition

7. A record is “information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business[1]”.

Records Lifecycle

8. The key life cycle phases of a record are:



[1] International Standards Organisation ISO 15489 Information and documentation: Records Management, Part 1 2001

Phase 1 - Creation and Receipt

9. It is your responsibility to ensure all records are filed in an appropriate manner, following records creation procedures.

10. This handbook, together with the Information and Records Management Policy, File Plan and Retention Schedule and other related policies and procedures form the records management system. This system:

    (i) accommodates both paper file systems and records that are created or exist in electronic format

    (ii) provides a simple information structure for logical file storage

    (iii) provides referencing and classification metadata for effective retrieval of accurate and related information

Record Storage & Indexing

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

12. 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 and logically indexed are easier to manage to meet these requirements.

13. To this end you must index all records you create and records you receive from outside the organisation with the applicable system metadata as stipulated in the relevant indexing procedures and guidelines.

Phase 2 – Maintenance and Use

14. Throughout the lifecycle of a record you must ensure that the metadata remains current and appropriate.

15. This is particularly important when working with Key Documents which are managed following specific procedures and guidance, as set out in Management and Review of Key Documents Handbook.

Phase 3 – Review and Retention

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

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

Phase 4 – Disposal

18. 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.

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

Section 3 - Hardware

Desktop PCs and Laptops

20. You will be provided with a desktop personal computer (PC). The PC will be connected to the SIC network servers with access to the internet, email, network drives and the necessary software required according to your role.

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

22. There are encrypted laptops for use by staff when in the office, working from home or attending events or meetings. If you are working from home, you must always use an encrypted laptop provided by CST. Members of the SMT are provided with encrypted laptops or tablets.

23. You should obtain permission from your line manager before CST provides you with a laptop. CST will complete the necessary paperwork before the equipment is removed from the office.

24. You must take all necessary precautions to safeguard the laptop and its contents. The following must be adhered to:

    (i) if travelling by car, the laptop must be locked in the boot and never left in plain sight

    (ii) the laptop must never be left unattended when using public transport or attending an event or meeting

    (iii) where a privacy screen and/or a security lock have been issued, these must be used to maintain confidentiality and security e.g. when the device is being used on public transport; when the device is being kept in a hotel

    (iv) only you may use it

    (v) the laptop can be connected to external internet access but this must be a secured network e.g. a home internet which is password protected

    (vi) do not connect the laptop to any external wired/wireless internet access in a public place e.g. a café. This connection is not secure and runs the risk of introducing viruses to the laptop

    (vii) the rules at section 12.5 of the Employee Handbook, Policy on the use of the Internet and Email, also apply to using the internet on the laptop

    (viii) do not download any software to the laptop – if you require specific software discuss this with your line manager

    (ix) each laptop is encrypted and requires passwords to access. Any password/s given to staff to access the laptops must not be divulged

    (x) the documents you require to work on should be transferred to the laptop prior to taking it out of the office using one of the memory sticks available from CS

    (xi) before returning the laptop to CST ensure that you have transferred your work from the laptop to your desktop computer using an CST memory stick and deleted it from the laptop, including emptying the Recycle Bin.

25. Any theft or loss of a laptop (or any other equipment) removed from the office must be reported immediately to the HOCS.

26. Viruses can be introduced into the SIC network or transmitted to a third party's system by sending and receiving e-mail and by using the internet. You must take all reasonable steps to ensure that no viruses are transmitted by you to any third parties and to ensure that you do not knowingly allow a virus to affect the SIC computer systems:

27. To maintain security the network firewall may prevent access to some websites. If you require access to a blocked site for business use you must first seek the HOCS' permission. If given, the HOCS will instruct CST to 'whitelist' the site.

28. 'Zip files', which usually enter the network as attachments to emails, have a high risk of carrying a 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 :

    (i) if you know it is SPAM, delete the email and attachment immediately, or.

    (ii) if you believe the attachment is genuine, confirm the sender's identity by calling them (preferred), or by email. 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, ask the sender to password protect the zip file. If these options are not possible, refer to the HOCS for permission before accessing the zip file.

Hardware - Other

SIC Memory Sticks

Memory Sticks

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

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

31. You must ensure that memory sticks (both encrypted and un-encrypted) remain secure at all times.

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

Encrypted Memory Sticks

33. If you need to take sensitive and/or confidential information out of the office e.g. attending an external meeting, you should take this information loaded onto a SIC laptop. On the very rare occasion where a laptop is not available an encrypted memory stick is available from CST.

34. In order to access the information contained on the 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.

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

Un-encrypted Memory Sticks

36. Information which is on an un-encrypted memory stick being removed from the office must not be confidential/sensitive in nature e.g. a presentation could be saved in this way.

Non SIC Memory Sticks (and other media)

37. We may be sent information on a memory stick or other media, such as CD. Examples include a presentation or withheld information from a public authority.

38. Your PC is 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

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

Software provided by SIC to manage records

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

System	Definition
ACT!	Day to day records of communication between SIC and external agencies and individuals that do not form part of cases managed using Workpro
Workpro	Case records related to individual applications for decision, complaints, requests for information, authority assessments, publication scheme approvals, enquiries, and enforcement action
Virtual Cabinet (VC)	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 SIC 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

41. 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.

42. 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

43. All information on network drives forms part of the SIC's corporate records and must be managed according to this handbook and any additional guidance provided.

44. You have access to network drives depending on your role e.g. only CST has access to the S:drive for Sage[2] financial data.

P:drive – Public drive

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

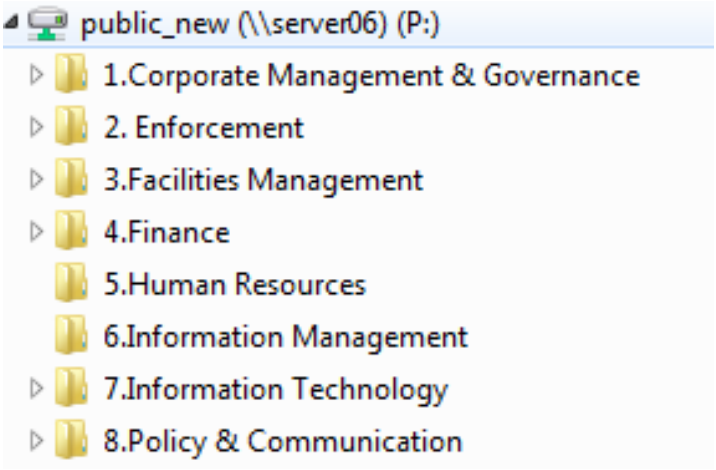
    (i) storage for pictures and images used by the Policy and Information Team

    (ii) spreadsheets which cannot be linked together in VC

    (iii) Workpro templates – master copies for uploading to Workpro

    (iv) 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.

46. 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.



47. 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.

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

49. A Staff Sharing Folder has been created as an area where you can temporarily share non-work information with colleagues e.g. pictures of a wedding or holiday.

50. If you share information using this folder it is your responsibility to ensure that the information is deleted after one month. The contents of this folder are part of our daily back-up and will be part of routine reviews of information held as part of our Retention Schedule.

[2] 'Sage' – accounting software package

Z:drive

51. The SIC recognises that, exceptionally, there may be occasions when staff wish to have information which does not form part of the SIC'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.

52. 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.

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

    (i) Colleagues may not have access to the necessary up-to-date information should you be off unexpectedly

    (ii) Records are not stored appropriately in line with the file plan

    (iii) Version control, destruction of records and retention schedule cannot be adhered to

    (iv) Records could be inadvertently missed as part of a search in response to an information request.

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

55. 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).

56. 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

57. 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

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

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

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

O:drive

61. The O:drive is only visable to staff who have access to ACT! software.

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

E:drive

63. The SMT and FAM have access to the E:drive which is used for spreadsheets which cannot be linked within VC.

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

PC – C:drive

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

66. You must use the appropriate software, network drive or, (in the case of laptops) a memory stick, for saving documents.

PC – Desktop

67. Your desktop is linked to your roaming profile (see below) and has the shortcuts to the programs you use. The 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.

68. 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.

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

70. The risks described at paragraph 53 also apply to the desktop.

71. The files on your 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.

Your IT Account (Roaming Profile)

---

72. When starting employment with the SIC each staff member is provided with an IT account allowing access to SIC network. This account is also your ‘roaming profile’.

73. You are responsible for any action carried out under your IT account. To avoid misuse, you should lock your workstation when away from your desk and you must never divulge your

password to anyone. 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.

74. Each time you log on with your username and password to a PC or laptop (connected to the network) it will load your roaming profile. This allows you to work at any PC and laptop within the office and still have access to your own desktop, emails and documents.

75. Your roaming profile contains the following information:

    (i) Username and password

    (ii) Contents of desktop – shortcuts, files and Recycle Bin

    (iii) Microsoft Outlook – all email folders and contents

    (iv) Contents of My Document

    (v) Contents of My Videos

    (vi) Contents of My Pictures

    (vii) Contents of My Music

    (viii) Contents of Downloads folder.

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

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

Section 5 - Managing Email Messages

Introduction

78. 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, FOISA and the EIRs.

79. To manage email messages you need to distinguish between email messages that are records of business activities (records), and those that are ephemeral email messages. You must move records from personal mailboxes[3] to ensure they are managed with, and in the same way as, other records.

80. In exceptional circumstances it may be necessary to use personal email accounts for SIC business. 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.

81. Line-management authorisation must be sent to the email address being used, copied to the individual's SIC account, the line manager's SIC account and the Head of Corporate Services's (HOCS) SIC account before any other emails are exchanged.

82. All emails sent to or received by a personal email account must be copied to the individual's and line manager's SIC accounts.

83. 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.

84. The HOCS will monitor to ensure that confirmation of the deletion of emails held on personal accounts is received.

85. SIC information held in a personal email account will be regarded as information held by the SIC and will fall within the scope of requests for information received by the SIC. Section 65 of FOISA and regulation 19 of the EIR's apply to this information.

86. Your personal mailbox within Outlook will be 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.

87. 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.

88. The Employee Handbook includes an Email and Internet Policy which you must also adhere to.

[3] 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

89. 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.

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

    (i) Identifying email records

    (ii) Who is responsible for capturing email records

    (iii) Email messages with attachments

    (iv) When to capture email records

    (v) Where to capture email records

    (vi) Subject of email records.

Identification

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

92. 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?

93. 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
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

94. 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.

95. 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

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

97. Email messages that constitute records must be saved to the appropriate software - ACT!, VC or Workpro.

98. 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).

99. 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

100. 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.

101. 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

102. By default your personal Deleted Items folder will be emptied when you exit Outlook.

103. 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.

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

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

Good Practice: Making your Mailbox Manageable

106. Managing an email mailbox effectively can appear to be a difficult task, especially if a large volume of email messages is received regularly. It should not be about following rigid classification guidelines; it is about following a methodology that works best for you.

107. 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. 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

108. Colleagues may need to access email messages from your mailbox when you are away from the office for an extended period, for example holiday or sickness e.g. to respond to an information request or to an enquiry from an applicant.

109. See the Email and Internet Policy contained within the Employee Handbook.

110. 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.

111. 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).

112. 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)

113. 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.

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

115. It is the responsibility of the identified owner to establish procedures for the management of the shared mailbox, and to communicate them to others who have access to it.

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

116. There are a 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.

117. 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.

118. 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.

119. 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 they 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

120. 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:

    (i) Identifying an owner

    (ii) the purpose

    (iii) access

    (iv) managing the contents of shared mailboxes and public folders.

121. 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.

122. 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.

123. 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.

124. 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.

125. 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.

126. The default access to all public folders is that Administrators can view the contents of all the folders.

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

Introduction

127. 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, FOISA and the EIRs.

128. 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

129. 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

130. 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. CDs)). 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.

131. Secure Store – used for storage of confidential documents and governance and finance records required for the operation of SIC, 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 SIC), 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.

132. 'Bell' – the CST create and hold some records in paper format to fulfil the operational functions of SIC, such as hard copy personnel files, recruitment records, and bank statements. 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.

133. 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

134. 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

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

136. You should ensure that you 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

137. 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. Further guidance is provided in the VC User Manual which is accessed by clicking the  in the top right corner of VC.

138. 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

139. 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!

140. 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

141. 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

142. 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:

    (i) Description – meaningful description of record, including naming convention where appropriate

    (ii) Document Author – SIC staff member creating new records or capturing records from external source

    (iii) 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 144)

    (iv) 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 144)

    (v) Document Types - refer to the format or layout of the documents being filed.

What if I have problems indexing a record in VC?

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

144. 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, update the original document.

VC– Guidance on Naming Conventions

145. Take the time to provide a concise and reliable description for a document 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).

146. Presume a future searcher has no prior knowledge about the document you are naming or describing, e.g. a procedure document about naming documents in VC, should be called something like "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".

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

148. 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".

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

150. 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 elsewhere in the fields (such as the revision field) or in the document itself.

151. Do not use abbreviations or numbers, or meaningless classification schemes in the description field – e.g. Budget SIC 2012-13 Original CE which would mean nothing to a newcomer to the organisation.

152. 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. 2009 09 26
- Month – YYYY MM e.g. 2009 09
- Year – YYYY e.g. 2009
- Range of years – YYYY – YY e.g. 2009 – 10

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

154. Which system "owns" the master organisation list?

(i) Scottish Public Authorities – Workpro

(ii) SIC Suppliers – SAGE

(iii) All other external organisations – ACT!

155. 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. 2009 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 adhoc, a brief meaningful description of the meeting should be used.
	Meeting Agenda	YYYY MM DD [Meeting name] Agenda e.g. 2009 11 03 QSMTM Agenda	

VC –Individual Functions

156. 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]	
	Project	YYYY MM DD [meaningful description]	A subject for each project will be created – it will show which Operational Plan activity it relates to, the name of the project, and the project manager's initials e.g. 'IM7 – Records Management (DL)'
Enforcement			
Investigation	Draft Decision Notice	Draft Decision Smith and Scottish Information Commissioner 201301234	
Investigation	Final Decision Notice	YYYY MM DD Decision 123/2013 Smith and Scottish Information Commissioner 201301234	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	YYYY MM DD Decision 123/2013 ANON Smith and Scottish Information Commissioner 201301234	Should be created from the final version of the draft and should only have 1 version. Date is the date of issue.
Practice Recommendation		Draft Practice Recommendation Scottish Ministers EN80006	
Practice Recommendation		YYYY MM DD Practice Recommendation Scottish Ministers EN80006	Should be created from the final version of the draft and should only have 1 version. Date is

Filing Location/Activity	Record type	Convention	Notes/keyword selection
			the date of issue.
Enforcement Notice		Draft Enforcement Notice Scottish Ministers EN80006	
Enforcement Notice		YYYY MM DD Enforcement Notice Scottish Ministers EN80006	Should be created from the final version of the draft and should only have 1 version. Date is the date of issue.
Enforcement / Management of Enforcement Function / Quality and Performance Management			
Quality Assurance	Completed forms	YYYY MM DD [Name of Assessor/Officer] [Name of form] [WP reference] e.g. 2014 10 01 EM/GW QA Records Management 201400099	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. 2008 06 01 to 2009 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 & Expenses	Expense claims	YYYY MM Expenses Claim [staff initials] e.g. 2008 08 Expenses Claim JS	
Procurement/ Contract Management	Contracts	YYYY MM DD to YYYY MM DD [subject of contract] contract e.g. 2008 06 01 – 2009 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			

Filing Location/Activity	Record type	Convention	Notes/keyword selection
		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			
		2013 Timesheet J Smith	
Information Management			
		YYYY MM DD [meaningful description]	
Information Technology			
		YYYY MM DD [meaningful description]	
Policy and Communication			
Publications and Guidance	Decisions Round-up	YYYY MM DD Decisions Round-up DD MONTH to DD MONTH YYYY e.g. 2014 05 16 Decisions Round-up 12 to 16 May 2014 OR 2014 05 02 Decisions Round-up 28 April to 02 May 2014	First date is the date of publication on the website

Workpro - Guidance for indexing and filing documents and folders

157. 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”.

158. The Investigations Handbook contains guidance on naming documents, in particular Section 1: Receipt and validation of applications.

159. 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.

160. When sending email messages with attachments to Workpro always mark clearly to show that there are attachments and how many there are e.g. Email from App + 3 attachments

ACT! - Guidance for indexing and filing documents and folders

ACT! – Guidance on Naming Conventions

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

    (i) Date is in the format YYYY MM DD at the start of the description

    (ii) Titles are concise and meaningful

162. If saving several emails regarding the same topic either:-

    (i) save the final email with the full string of the conversation, appropriately renamed; or

    (ii) 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

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

164. The Information and Records Management Policy, Section 2 requires that SIC's records are:-

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

- *Ensure that the correct records are held by the SIC for the:*
    - *conduct of business*
    - *maintenance of corporate memory*
    - *development of a knowledge base of skills and experience.*
- *Support the SIC Records Management 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 SIC'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 SIC does not need and may lead to non-compliance with the FOISA, the EIRs and the DPA and possible legal action against the organisation.*
- *Ensure accurate indexing of records."*

165. In order to comply with the requirements of the Information and Records Management Policy the SIC ensures that a review of all records held is carried out on an annual basis for each function.

Review Planning

166. The reviews are staggered throughout each year with the schedule being informed by and set through the Operational Plan planning process in January of each year.

167. Each team within the organisation (Corporate Services, 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	
Corporate Management and Governance	Quarter 3 (October – December)
Facilities Management	
Finance	
Information Management	
Information Technology	
Human Resources	
ACT! records	Quarter 4 (January – March)

168. Custodians should refer to the Records Review Procedures for guidance in carrying out a review of records.

169. Documentation which supports the information and records management process within SIC is reviewed annually in Quarter 4.

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

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

171. 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

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

Disposal of Paper Records

173. The SIC operates a 'shred all' policy and has in place a contract to carry out the secure onsite destruction of all waste paper.

174. 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.

175. Section 34 of the Environmental Protection Act 1990, as detailed in the Code of Practice[4] requires those subject to a Duty of Care to keep records of the waste they receive and consign i.e. a Waste Transfer Note. SIC maintains a Waste Transfer Note which is renewed annually.

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

Section 8 - Disposal of IT Equipment

176. Obsolete IT assets, usually PCs, servers, laptops and the hard discs therein, are generally disposed of due to obsolescence rather than being surplus to requirement. These should not be offered for sale, but disposed of securely to ensure the security of data held on the disc is not compromised.

177. A fixed asset disposal approval form (Appendix A of the Finance Policy - Fixed Assets) must be completed for each piece of equipment that is being disposed of.

    (i) Complete all fields and attach a copy of the original invoice.

    (ii) Be clear what will happen with the devices being disposed of.

178. Each fixed asset disposal approval form must be signed by the HOCS, giving approval to dispose of the equipment.

179. Wipe clean the hard discs using software recommended by SIC's external IT service provider (Instructions in the IT & Telephone Manual).

180. Contact disposal service providers to arrange secure disposal of equipment.

- Obtain quotes from at least 2 providers, asking for details of the following:

    (i) Security accreditation

    (ii) Security and tracking on vans

    (iii) Staff screening

    (iv) Their own security audit process

    (v) Compliance with WEEE Regulations 2013

    (vi) What happens to hard drives – possible to shred hard drives at OSIC?

    (vii) What happens to other parts of the pc/server/laptop - destroyed/recycled/reused?

    (viii) Confirmation that Certificates of Destruction will be provided for each individual piece of equipment.

- Be aware that any specialist service provider will be considered to be a 'data processor' under the DPA.

181. Before any IT assets are disposed of a signed contract must be in place to ensure that:

    (i) There is an appropriate level of security in place (Para 15 of the Data Protection Policy)

    (ii) Explicit directions on the services to be undertaken are given.

182. Where possible, hard drives should be shredded on site.

183. Produce a list of equipment to be taken off site by the service provider and ask them to sign the form to confirm what equipment they are removing.

184. Ensure the service provider provides Certificates of Destruction for all component parts of equipment showing serial number and method of destruction.

185. Certificates of Destruction must be scanned into VC and the hard copy kept with the Fixed Asset Disposal Form in the Fixed Asset Folder in Bell Cupboard.

186. 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:

    (i) Assess the risks associated with the breach, and

    (ii) Inform the appropriate people and organisations that the breach has occurred

    (iii) Investigate the cause of the breach and evaluate the effectiveness of our response. If necessary, update our 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 and RMT representatives
- Monitors levels of compliance to the IRM Policies and associated procedures
- Communicates IRM Policies and Procedures by all appropriate means
- Ensures the provision of information management training for all staff
- 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
- 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 SIC 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 support 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 support tools e.g. ARMS

Role:
Administrator

Function:
Information and Records Management Support

Summary Description:
Providing operational support for IRM function

Responsibilities:

- Administration of the different IRM systems within the SIC
- Assist SIC 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 colleagues in relation to IRM systems, processes and procedures, with support of third parties where required
- Monitor review and disposal activities, and assist the Records Custodians with carrying out timely destruction of expired documents and records
- Provide induction training in IRM policies, procedures and systems
- Maintain register of non-investigation paper records
- 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 SIC 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 SIC 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 support of 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:
Representatives from the Enforcement, Corporate Services and Policy & Information teams

Function:
Records Management Team

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

Responsibilities:

- Facilitation role between SIC teams and the HOCS
    - Represent their team's interests on the RMT
    - Communicate progress, decisions and required actions related to IRM function within their team
    - Feedback information management issues raised by their team to the RMT Group
- 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	Regular internal 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 SIC IRM Policies, Procedures and Processes and can explain them to others	Regular internal 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 SIC and manage those records in keeping with the IRM policy and associated procedures and guidance

Responsibilities:

- Has understanding of 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 information keeping 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 of no significant operational, informational or evidential value requiring its retention as soon as it has served its immediate purpose.

Required Core Skills & Training Methods:

Core Skill	Training Method
Understanding of basic IRM concepts and requirements	Induction training
Understanding of the different IRM systems within SIC – 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 SIC IRM Policies, Procedures and Processes	Induction and regular internal training

Section 10 – Data Protection

Compliance Monitoring

187. The Data Protection Policy sets how we comply with the requirements of the Data Protection Act 1998 (DPA).

188. It gives the FAM the responsibility for:

(i) ensuring that SIC's Data Protection Notification is kept up to date

(ii) in conjunction with the SMT, reviewing and updating DPA procedures as necessary

(iii) monitoring compliance with DPA policy and procedures.

189. The following table details how the FAM will monitor compliance with the DPA, and our policy and procedures. The outcomes of these checks will determine what changes, if any, need to be made the DPA procedures.

	Document title	Compliance Check	Review Frequency
1	Data Protection Policy	Review of compliance with legislation and ICO guidance Update to ensure it reflects current SIC practice & procedures	Per Register of Key Documents
2	Information and Records Management Policy	Review of compliance with legislation and ICO guidance Update to ensure it reflects current SIC practice & procedures	Per Register of Key Documents
3	Records Management Plan	Review of compliance with legislation and ICO guidance Update to ensure it reflects current SIC practice & procedures	Per Register of Key Documents
4	Employee Handbook	Annual compliance check with Law at Work to provide assurance on DP matters Check sample of HR files (paper and electronic)	Annual
5	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)	Annual
6	Information Requests / SARs	Review sample of SAR and S1 responses	Annual
7	Enquiries Procedures	Review of sample of files active during review period	Two Years
8	File Plan & Retention Schedule	Review retention periods for records containing personal data	Two Years
9	Investigations Handbook	Review of sample of files active during review period	Two Years

10	Recruitment Policy & Handbook	Review of all files (electronic and paper) active during review period	Two Years
11	References Policy	Review of all references supplied during review period	Two Years

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

191. The FAM will prepare a report of the DP compliance checks undertaken each year, which will be incorporated in the annual report on Records Management in line with the SIC's governance arrangements.

Personal Data Breaches

192. The ICO describes a personal data breach as any security incident that affects the confidentiality, integrity or availability of personal data. A breach will include situations where personal data are:

    (i) lost or corrupted;

    (ii) altered, destroyed, accessed or disclosed without proper authority;

    (iii) made unavailable, for example by encrypted ransomware.

193. A personal data breach can happen for a number of reasons, both accidental and deliberate:

    (i) Loss or theft of data or equipment on which data is stored

    (ii) Inappropriate access controls allowing unauthorised access

    (iii) Equipment failure

    (iv) Human error

    (v) Unforeseen circumstances such as fire or flood

    (vi) Hacking attack

    (vii) 'Blagging' offences where information is obtained by deception.

194. Our policies and procedures, supported by the compliance checks described above, are designed to minimise the risk of personal data breaches occurring.

195. However, in the event that a personal data breach (or a near-miss) does occur**, it must be reported immediately to the FAM** (in whose absence, the HOCS, which failing another member of the SMT). The FAM will prepare a briefing note as a matter of urgency and then immediately report the event to the HOCS. The briefing note, related correspondence and any Breach Management Plan will be held in VC with the security profile "Management and FAM".

196. Where a processor (e.g. a contractor processing personal data on our behalf) detects a personal data breach in relation to our data, it should report that breach to the FAM as soon as possible.

197. The FAM, under the guidance of the HOCS, will initiate a Breach Management Plan (BMP), which comprises four steps:

    (i) Containment and recovery

(ii) Assessment of ongoing risk

(iii) Notification of breach

(iv) Evaluation and response

198. BMP guidance and a Data Breach form can be found as a single Word document in VC templates, and follows the ICO's Guidance on Data Security Breach Management.

This ICO Guidance reflects the requirements of the Data Protection Act 1998. Much of it is still relevant following the coming into force of the General Data Protection Regulation (GDPR) and the Data Protection Act 2018, but the relevant section of the ICO's Guide to the GDPR should be followed in relation to notifying the ICO and data subjects about a breach:

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

If you have any questions about what to do or need any further information please speak to the HOCS or the HOE.

199. Each security breach or near-miss will be distinct in nature and require a different response. It is therefore not possible to be prescriptive about the detailed response to each occurrence. However, applying the ICO's guidance will ensure that our response to an occurrence is appropriate.

200. In all cases, we must bear in mind the need to consider whether the personal data breach needs to be notified to:

(i) The ICO. We must do this for every breach, unless we're satisfied that the breach is unlikely to result in a risk to anyone's rights and freedoms (consideration of this needs to be documented, in the "Assessing the risks" section of the BMP). In every case where we do need to notify, we must do so within 72 hours of becoming aware of the breach.

For ICO contact arrangements, see

https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/).

(ii) The data subject(s). We must do this where a breach is likely to result in a high risk to the rights and freedoms of the individual(s) concerned. This means the "Assessing the risks" section of the BMP also needs to consider the severity of any potential impact and the likelihood of it occurring. Where a high risk is identified, we need to inform the affected individuals as soon as possible, unless we're satisfied that we've either –

(a) applied appropriate measures (e.g. encryption) to protect the affected personal data and render them unintelligible to unauthorised persons, or

(b) taken measures following the breach to ensure that the high risk is no longer likely to materialise.

201. Notification to the ICO must include details of:

(i) the nature of the breach, including (where possible) the categories and approximate number of affected –

(a) data subjects and

(b) personal data records;

- the name and contact details of the Data Protection Officer (DPO) or other contact point where the ICO can obtain more information;
- the likely consequences of the breach;
- the measures we are taking or propose to address the breach, including any measures to mitigate its possible adverse effects.

(Where we can't provide all of this within the 72 hours, we provide what we can – with an explanation of the delay – and follow it up with the rest as soon as possible.)

202. Notification to data subjects must include, in clear and plain language:

(i) a description of the nature of the breach, and

(ii) the information set out in 10(ii), (iii) and (iv) above.

Where we conclude that identifying, locating and contacting the affected individuals would involve disproportionate effort, we should make a public communication with the above information. Where we are processing the personal data in question for law enforcement purposes (e.g. for investigating a potential offence under section 65 of FOISA), we may restrict the information we give the data subject, to the extent necessary to avoid obstructing any related investigation or prosecution.

203. Given the relatively short timescale for notifying the ICO, it's important that consideration is given as soon as possible to whether we need the DPO's assistance in handling the breach. When notifying the ICO, we need to give contact details for the DPO or another appropriate point of contact, to allow the ICO to obtain more information on the breach – if the DPO is to be the contact, they must be fully informed about the breach before notification.

204. The DPO contact details are:

Email: DPOservice@parliament.scot

Telephone: (0131) 348 6080.)

205. Once the immediate issue has been responded to, the HOCS will provide a Committee Report to the SMT within 5 working days which will:

(i) describe the personal data breach (or near-miss)

(ii) detail what steps were taken to comply with the GDPR and the ICO's guidance

(iii) make recommendations for any changes to procedures which will avoid, or reduce the risk of, a re-occurrence.

206. The BMP and the Committee Report (with records of any relevant SMT decision(s) and of the implementation of any relevant actions/decisions) must be retained as a formal record of the breach. and must be filed in VC with the security profile "Management and FAM".

Appendix - 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 v02 CURRENT ISSUE
VC FileId	85931
Type	Procedure
Approver	SMT
Responsible Manager	HOCS
Date of next planned review	03/2020
Approval & Publication	
Approval Date (major version)	29/03/17
For publication *(Y/N)*	Y
Date published	25/06/18
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	28/05/18

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*)
30/03/17	KB	03.00	03.01	New version created following planned review
30/03/17	KB	03.01	03:02	DCS updated, published on website
06/07/17	KB	03.02	03.03	Amended reference to CST, corrected typos, updated O:drive guidance
12/07/17	KB	03.03	03.04	Update para 158
25/05/18	EM	03.04	03.05	Revised section on personal data breaches
25/05/18	HGS	03.05	03.06	Changes approved and DCS updated
25/05/18	LB	03.06	03.07	DCS updated and document published
28/05/18	EM	03.07	03.08	Paragraph 202 (data breaches) further updated
25/06/18	KB	03.08	03.09	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