Scottish Information Commissioner Records Management Plan – Evidence Extracts

www.itspublicknowledge.info

Contents

Records Management Plan – Evidence Schedule

Items highlighted in grey have been appended below

Element		Evidence – Source Document	Evidence - Details
1	Senior Management Responsibility	Records Management Plan	Covering Statement – page 3
		Information & Records Management Policy	Section 3 - Roles & Responsibilities
2	Records Manager Responsibility	Records Management Plan	Covering Statement – page 3
		Information & Records Management Policy	Section 3 - Roles & Responsibilities
		Information & Records Management Handbook	Section 8 – Competences Framework
3	Records Management Policy Statement	Information & Records Management Policy	Whole Policy
4	Business Classification	File Plan & Retention Schedule	Part 1 – File Plan
5	Retention Schedules	Information & Records Management Policy	Section 2 – Review, Retention & Disposal
		Information & Records Management Handbook	Section 7 - Review and Disposal of Records
		Records Review Procedures	Whole Procedure
		File Plan & Retention Schedule	Part 2 – Retention Schedule
6	Destruction Arrangements	Information & Records Management Handbook	Section 7 – Review and Disposal of Records
		Records Review Procedures	Whole Procedure

Element		Evidence – Source Document	Evidence - Details
		Information & Records Management Policy	Section 2 – Review, Retention & Disposal
		File Plan & Retention Schedule	Part 2 – Retention Schedule
		6.1 – Certificate of Destruction – paper records	Sample Certificate
7	Archiving and Transfer Arrangements	Memorandum of Understanding between the Keeper and SIC	Whole Memorandum of Understanding
8	Information Security	Information & Records Management Policy	Section 6 – Information Security
		Information & Records Management Handbook	Section 3 – Hardware Section 4 –Software etc. Section 7 – Review and
		8.1 - Employee Handbook (extract)	Disposal of Records Section 4.1 – Confidentiality and official information
		8.2 - Employee Handbook (extract)	Disposal of Records Section 12.5 – Policy on the use of the Internet, Email and Other Business Communications Systems
		8.3 - Risk Register (extract)	Risk relating to information security
		8.4 - Staff Manual (extract)	Clear desk policy
		8.5 - Investigations Procedures (extract)	Section 13 – Records Management
		8.6 - Certificate of Destruction – IT	Sample Certificate
9	Data Protection	Data Protection Policy	Whole Policy

Element		Evidence – Source Document	Evidence - Details
		9.1 - Employee Handbook (extract)	Section 12.3 – Data Protection Policy in relation to Employee Information
		9.2 - Enquiries Procedure (extract)	Section 5 – Subject Access Requests
10	Business Continuity and Vital Records	10.1 - Business Continuity Plan (extract)	Section 1 – Day 1 to 6 Action Plan Section 2 – Core Recovery Team Contents Page
11	Audit Trail	Information & Records Management Policy	Section 4 – Performance Review and Compliance Monitoring
		Information & Records Management Handbook	Section 6 – Records Storage, version Control, Naming Conventions & Indexing
		Records Review Procedures	Whole Procedure
		11.1 - INVU destruction log (extract)	Sample log
		11.2 - Paper destruction log (extract)	Sample log
12	Competency Framework for Records Management Staff	Information & Records Management Policy	Section 3- Roles and Responsibilities
		Information & Records Management Handbook	Section 9 - Competences Framework
		12.1 - Head of Operational Management Job Description (extract)	Records Management Responsibilities
13	Review and Assessment	Governance Reporting Arrangements	Whole Document
		Management and Review of Key Documents	Whole Procedure

Element		Evidence – Source Document	Evidence - Details
		13.1 - Operational Plan 2013/14 (extract)	Information Management Section
		Information & Data Management Review Report	Whole Report
14	Shared Information	Data Protection Policy	Whole Policy
		Publication Scheme – Guide to Information	Whole Guide

Element 6 - Destruction Arrangements

6.1 - Certificate of Destruction – paper records

Shred-it

Shred- it
161 Cocklaw Street
Kelty
FIFE
KY4 0DH
Phone: 01383838313

SERVICE RECORD SUMMARY
CERTIFICATE OF DESTRUCTION
PLEASE KEEP THIS FOR YOUR RECORDS
(THIS IS NOT AN INVOICE)
EWC Code: 200101
SIC Code: 80.10
We the producer have discharged our duty to comply with the hierarchy of waste management

Customer: 0012550285
SCOTTISH INFORMATION COMMISSIONER
BLD:KINBURN CASTLE
DOUBLEDYKES ROAD
ST ANDREWS KY16 9DS

Order #: 8010509418
Order Date: 20.01.2014
Service Type: SHRED - ON- SITE AUTOMATIC

Contact: JAN WALLACE

Time In: 08:32 AM

Material Collected	
WHITE BAG	**7**
Total:	**7**

Service Time:	**13 Min**
Number of Equip Serviced:	**3**
Number of Extra Items Collected:	**7**

Customer Signature: K BERRY

[redacted]

CSR Signature [redacted]

Element 8 – Information Security

8.1 - Employee handbook (extract) – Section 4.1

Section 4.1 - Confidentiality and official information

1. The Commissioner is committed to making OSIC open, accountable and transparent. The Commissioner's Publication Scheme provides a list of all available information about the Commissioner and OSIC and how to get it. Wherever possible, information will be provided on the website www.itspublicknowledge.info.

2. The Commissioner and her staff will also make available information about their contacts where it is not exempt from disclosure under Part 2 of FOISA. In the case of public bodies, the information to be made available is likely to include information such as names of contact people, copies of correspondence and links to their website. In the case of the public, this is likely to include names of people or organisations who have applied to the Commissioner for a decision, although where names are published this will usually only happen after the decision has been published.

3. The Commissioner has a duty under FOISA and the EIRs to make decisions as to whether public authorities have complied with the legislation. This involves accessing information held by public authorities which they consider to be exempt or excepted from disclosure. Section 45 of FOISA (which also applies to investigations etc. carried out under the EIRs) makes it a criminal offence for the Commissioner and OSIC staff to disclose, without lawful authority, information which has been obtained by or furnished to the Commissioner for the purposes of FOISA and the EIRs and which is not, or has not been, otherwise publicly available. You must not, therefore, knowingly or deliberately take part in activities or make public statements which might involve the disclosure of such information, or in any other way disclose it contrary to section 45 of FOISA.

4. The Commissioner may disclose information gathered in the course of an investigation to the Scottish Public Services Ombudsman if that information could be the subject of an investigation by the Ombudsman. The Commissioner may also release information gathered in the course of an investigation to the Information Commissioner.

5. Further to this, you have a contractual duty not to misuse information that you acquire in the course of your work or disclose information that is received in confidence from others. This applies even after you leave the Commissioner's employment.

6. Nothing in this policy is intended to prevent you making a protected disclosure under the Public Interest Disclosure Act 1998.

8.2 - Employee handbook (extract) – Section 12.5

Section 12.5 - Policy on the use of the Internet, E-mail and Other Business Communications Systems

Scope

146. This policy applies to all OSIC staff, staff on secondment and contractors who are authorised to use the Commissioner's internet, e-mail and other business communications systems. Any references to an "employee" or "staff" shall include staff on secondment and contractors who have been issued with a user account.

Principles on the use of the internet and e-mail systems

147. The principles under which you are authorised to use the Internet and e-mail systems are as follows:

- The Internet and e-mail are business systems. The Commissioner requires that all use of the systems by you is primarily for business purposes.
- You may, however, use the systems for limited non-business use if you do so in your own time, for example during your break or before or after work provided you observe the terms of this policy.
- You may also use these systems for personal purposes in the same way that short, important, personal telephone calls are allowed (see paragraphs 685 to 688below).
- The Commissioner may monitor and record the use of the internet and any e-mails which are transmitted over its computer system for the reasons set out in paragraphs 682 to 684 below. This means that you must not expect to have total privacy in respect of any messages you send or receive or in your use of the internet.
- All internet and e-mail use is automatically recorded by the IT systems and through these logs use can be attributed accurately to individual users. Normally we will only interrogate these logs for the reasons set out in paragraphs 682 to 684 below. However, in line with ICT security best practices, the Commissioner reserves the right to review these logs to ensure adherence to this policy.
- You are required to comply with this policy at all times. The consequences of failing to comply with the policy are set out in paragraphs 689 to 692 below. This means that all breaches in this policy will be dealt with under the disciplinary procedures.
- You must ensure you do not discriminate in respect of age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, gender identity, sexual orientation, trade union membership or lack thereof.
- Since the technology and law in this area are subject to change, this policy will be updated from time to time. The Commissioner will bring any updated policy to your attention before it is introduced.

Commercial and legal effects of e-mail

148. The commercial and legal effects of sending and receiving e-mails are the same as any other form of written communication. The style, tone and content of e-mails have a direct effect on the way OSIC, and indeed the Commissioner himself, is perceived by others. E-mails can contractually bind the Commissioner and any commercial advice, opinion, guarantee, representation or other statement contained in an e-mail may be relied upon by third parties.

149. You must not, therefore, send e-mails which make representations, contractual commitments or any form of legally binding statement concerning the Commissioner unless you have specific authority to do so.

150. It is your responsibility to ensure that appropriate records are retained in accordance with our corporate records retention schedule, including records of any commercial or legally binding e-mails which are sent in the course of OSIC business.

Security

151. You must take all reasonable steps to ensure that you do not unnecessarily compromise the security of the Commissioner's information and associated assets. 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. Unless you are an Administrator with authority to do so, you should never attempt to log on to, or use, a network account that is not yours.

152. Internet e-mail is not a secure means of transmitting information. It can be intercepted or can be sent to the wrong person or organisation. It can easily be copied and widely distributed. You should be aware of these hazards when you send emails.

153. All e-mails that are sent from the OSIC system automatically contain the disclaimer set out in Annex 1. You must not delete, alter or otherwise interfere with the automatic disclaimer.

Viruses

154. Viruses can be introduced into the OSIC network or transmitted to a third party's system by sending and receiving e-mail and by using the internet. The deliberate introduction of a virus onto a third party's computer systems may be a criminal offence. Accidental introduction of viruses on to a third party's computer system may, in certain circumstances, give rise to a claim against the Commissioner by that third party. 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 OSIC computer systems.

155. All e-mail transmitted via the OSIC network is automatically scanned for viruses whether it is being sent or received. Since a virus may, nevertheless, slip through, please beware of all unsolicited e-mails and e-mails from unknown sources. If you have any reason to be suspicious, contact an Administrator for assistance before opening the message or attachment. If in any doubt, do not open or run any attached file.

156. From time to time, you may receive e-mails warning of computer viruses, encouraging you to forward the e-mail on to others. These are usually hoax messages designed to overload computer systems. If you receive such a message, please do not forward it but contact an Administrator immediately.

Unauthorised Use

157. Unless strictly necessary for proper conduct of your duties, e-mail and the internet must not be used for the creation, transmission, downloading, browsing, viewing, reproduction or accessing of any image, material or other data of any kind which:

- is illegal
- is unacceptable to the Commissioner, including but not limited to:
  - sexually explicit messages, images, cartoons, jokes, or any other material of a sexual nature, (including nude or partially dressed men or women);
  - malicious gossip or inappropriate personal information about others;
  - inappropriate emotional responses to others, for example e-mails that contain an aggressive or abusive tone and/or content;
  - anything which may harass, provoke, demean, degrade, threaten, victimise or discriminate against anyone else or a group of people, particularly on grounds of gender, gender identity, sexual orientation, marital, civil partnership, family or part-time status, racial group (including colour, race, nationality, national or ethnic origin), religion, disability, age or trade union membership/non membership/activities or political belief;
  - material which involves the inappropriate use of social networking sites, blogs, instant messaging, newsgroups, bulletin boards or forums. Examples of inappropriate use include posting data which breaches the confidentiality of information relating to the organisation and/or colleagues, posting information relating to colleagues which could be considered discriminatory, engagement in online dialogue regarding colleagues which could be considered "cyber" bullying and use of the Commissioner's logo or corporate branding on a personal web page;
  - material which is, or is potentially, defamatory;
  - material which does, or is likely to, introduce viruses, worms, Trojan horses, or other unauthorised software into the Commissioner's computer system (see paragraphs 9-11 above);
  - material which is concerned with your own commercial enterprise or conflicts with the interests of the Commissioner;
  - material which may be of embarrassment to the Commissioner such as making insulting or untrue statements about a company or its employees, products or services, which could then be reported as the Commissioner's official opinion or
  - material which unnecessarily disrupts the work of colleagues.

158. This list is illustrative and not exhaustive. If you have any questions as to whether a particular activity is/is not permissible, you should ask your line manager before acting. You should also note that the prohibitions in this policy still apply even if the material is located on a part of the system which is personal or password protected.
159. It is also clear that bullying and harassment can occur by electronic means (see Anti - harassment, -bullying and -victimisation policy) and that such behaviour is not determined solely

on the content of such correspondence. The tone or style used when writing e-mails is also extremely important. All users must ensure that they avoid using a bullying tone or style when sending correspondence electronically.

160. These restrictions on the use of e-mail and the internet apply to both business (unless otherwise stated) and personal use. The Commissioner considers that it is important that all use is restricted in this way to avoid disruption in the workplace and embarrassment, distress or offence to others. Remember that what is offensive material is determined by the effect on the recipient, not how it is regarded by the sender.

161. It may not always be possible to avoid receiving unacceptable e-mails from others. If you receive such material you should delete it. If the sender is someone you know, you should ask them not to send such material in future. If you do not know the sender, you must not reply to the e-mail, rather you should contact an Administrator for advice. If the email is from within OSIC you should report the matter to your line manager who may wish to raise it at a higher level or with the HOOM.

162. It is also possible to enter internet sites carrying offensive material by accident, for example sites that contain pornographic, derogatory, defamatory or obscene material. If you enter such a site, such access will not be considered a breach of this policy if you immediately close your browser window and report the matter to your line manager.

163. You must not create, transmit, download or reply to chain letters, junk mail or unsolicited commercial or advertising materials. If you receive such e-mails you should delete them immediately and they should not be forwarded to anyone else, either externally or internally. If the e-mail is unsolicited, do not click on any "unsubscribe" link as this may simply confirm to the sender that your e-mail account is active.

164. You are not permitted to download any software, audio files, games etc. from the internet or to install or use any unauthorised software or hardware from home to use on the OSIC network unless such activity has been approved by your HOD. If you require any particular business related software, please submit a written request, with a full business case, detailing why the software is required.

165. You must not access or attempt to access anyone else's e-mail account without their permission. In emergency cases your line manager may authorise the Administrator to perform a password reset on your IT account.

166. You must not use e-mail or the internet to impersonate others or to forge messages or e-mail addresses. Where a message is sent on behalf of another person the message should make it clear that this is the case and should identify the writer and the sender.

167. You must not browse, access or use any internet site in any manner which breaches its published terms and conditions or download or store any material without reading and complying with any copyright or licence restrictions. In addition, you must not store any copyright material (e.g. audio or video files) on the OSIC IT system if it is not directly related to the business of the Commissioner.

168. You must not use information feeds (an internet site that provides automatic updates of selected information from a variety of sources, e.g. news pages) unless for legitimate business purposes. For example, a legitimate business purpose might be for the HOOM to have automatic updates from a site that provides an information service on employment issues.

169. Any unauthorised use of the Commissioner's business systems may lead to the sanctions set out in paragraphs 689 to 692 below being imposed.

Additional Guidance on the use of E-Mail

170. When using e-mail OSIC staff should remember the following:

- E-mail is a form of written communication. The generally recognised standards that apply to internal memos and external letters should be observed when sending e-mails.
- In line with Commissioner's Records Management policy and procedures, you should file all essential sent and received e-mails in INVU, Workpro or ACT! to create a record for ease of retrieval. You should delete all other messages (which do not require to be retained) on a regular basis.

Privacy and Monitoring

171. It is not the Commissioner's intention to monitor and/or record routinely any e-mails which are transmitted over the Commissioner's computer system or your use of the internet, including the nature of material downloaded from the internet. However, this information is automatically logged by the IT systems and we may, from time to time, monitor the systems for the following purposes:

- To ensure the Commissioner's practices, policies and procedures are being followed.
- To investigate or detect the suspected unauthorised use of the Commissioner's computer system.
- To secure the effective operation of the Commissioner's computer system.
- For the purpose of preventing or detecting crime.

172. If you are absent from work, or in the event of an emergency it may be necessary to check your inbox to ensure that mail items are dealt with appropriately in your absence. Under normal circumstances you will have given permission to another member of your team to access your inbox. However, there may be times when this is not possible and permission will be given to another work colleague. This will only be done if requested of the Administrator by your line manager. E-mails which are clearly personal or private will not be checked unless we have your prior permission.

173. This policy will be operated in line with the Commissioner's Data Protection Policy in relation to employee information.

Use of Office Telephones

174. The Commissioner recognises the occasional need to make short, important, personal telephone calls during work hours and expects you to use your personal mobile phone for these. However, the Commissioner's network may be used occasionally for such calls when this is not possible. You may not, however, may make personal use of international calls, unless:

- you are working abroad and have come to an arrangement with your line manager or
- you make arrangements to reimburse the cost of the calls.

Use of other Business Communications Systems

175. If you have been supplied with an office mobile phone, you may only use it for personal calls if:

- you have reached an agreement with your line manager as to what are reasonable personal calls or
- you inform your line manager and make arrangements to reimburse the cost of these calls, if they amount to more than £5:00.

176. You may also occasionally use the fax system for personal use.

177. You may not, however, under any circumstances, use the Commissioner's postage or stationery for personal purposes.

Breaches of the Policy

178. OSIC staff who breach this policy will be dealt with under the disciplinary procedures. If the breach is considered to be gross misconduct, the penalty will normally be summary dismissal without notice or compensation in lieu of notice. Offences include intentional viewing or downloading of pornographic or other derogatory, defamatory, obscene or inappropriate material.

179. Where a breach or an alleged breach of this policy involves harassment or discrimination, this may be reported or dealt with under the Anti-harassment, -bullying and -victimisation Policy at INV5152. Again, depending on the severity of the offence, the breach may be considered as gross misconduct.

180. Contract staff found to be in breach of this policy will be reported to the contract manager and may result in the abuser's services being terminated under the terms of the contract.

181. If we suspect that the Commissioner's business systems are being used for anything illegal, we will report these concerns to the police or any other relevant authority.

8.3 - Risk Register (extract)

Risk	Controls in Place	Action Planned
If the SIC does not have robust systems in place to ensure security of physical, human and information resources, it may be in breach of statutory duties (including committing criminal offence) and incur avoidable costs.	Text redacted	Text redacted

8.4 - Staff Manual (extract)

Clear Desk Policy

We have a clear desk policy. At the end of the working day desk surfaces should be clear of files, documents, publications, etc. These should be stored in your desk drawers or returned to the library. Other items should also be cleared away.

The reasons for this are:

- Security - to avoid material easily removable from desks being left lying about
- Access – to ensure that files / publications which may be required by other staff can be accessed in your absence
- Safety - to limit the potential damage to documents from spillage/ accidents
- Tidiness – to maintain a professional appearance to the office and to allow cleaning staff access to clean desks
- Cleaning – the cleaner will not clean any desk which is not clear.

8.5 - Investigations Procedures (extract) – Section 13

SECTION 13 - RECORDS MANAGEMENT

The Case File

13.1 Advice on saving information in WorkPro is contained throughout the procedures, but the following points give some additional information.

13.2 Information relating to an investigation must be kept safely and securely. Remember that it is a criminal offence to disclose information obtained in relation to an investigation without lawful authority.

13.3 As we have an electronic case management system for investigations, all correspondence received in connection with the investigation must be scanned in and saved under the relevant case file, or (for emails) forwarded to WorkPro and attached to the case file as soon as possible. Accurate records of all telephone conversations and notes from meetings must also be added to the WorkPro file at the earliest opportunity, so that an accurate, up-to-date record of the case is maintained.

13.4 All drafts of letters or emails which are not used should be deleted as soon as possible. It is the responsibility of the IO to ensure that both the electronic and the paper case file can be readily understood by DHOE, HOE and SIC. This includes ensuring that the documents in WorkPro are clearly named.

13.5 Once an application has been accepted as potentially valid, the VO will make up a paper file (see above). All hard copies of correspondence received in relation to the case should be filed in that file. As DHOE/HOE/SIC are likely to use the hard copy file when approving the decision, it is important that all items which need to be referenced in order to approve the decision are also retained in the hard copy file. However, the principle file is the file in WorkPro. There should be nothing relevant to the case kept in the paper file which is not kept in (or scanned into) the file in WorkPro, apart from documentary evidence – see 13.7 below.

13.6 The file made up by the VO will have the following information noted on the front of the file:

- name of applicant
- name of public authority
- name of IO (once allocated)
- case reference number (as per WorkPro)
- weighting and
- whether documentary evidence is being kept in a separate document box (see 13.7 below).

13.7 All documentary evidence which we receive from a public authority in support of their decision not to release information must be scanned in to WorkPro.

13.8 Where withheld information is received in an electronic form, the information and accompanying schedule must be saved in WorkPro, and a single hard copy of each placed in the WorkPro file, except in cases where it is impractical to do so. The WorkPro entry containing the

withheld information should be entitled, “INFORMATION WITHHELD/UNDER CONSIDERATION” (in upper case) to ensure that it is clearly identifiable within the file. If it is necessary to save the information within multiple entries (e.g. because the public authority provides more information at a later date), each entry must be clearly marked, but also numbered, e.g. “INFORMATION WITHHELD/UNDER CONSIDERATION (2)”. Once the information has been saved into the case file, the VO should ensure that any copies received, or forwarded, are deleted from email folders.

13.9 In some cases, the public authority will provide withheld information in paper form. Where this happens, the information will be scanned in along with the covering letter and schedule by Admin. The withheld information should be saved in a separate document, taking care to ensure that the order and alignment of the information matches the hard copy provided. The scanned file should be named by Admin, “withheld information 201xxxxxx”.

13.10 The VO must then save the letter, schedule and any withheld information into the WorkPro file. It is the responsibility of the VO to check that the scanned information matches the hard copy, and to arrange for it to be rescanned if any problems are identified. Once this process is complete, the VO will delete the information from any scanning folders and name the information in WorkPro as set out in paragraph 13.8.

13.11 If further information is identified for consideration during the investigation, the IO should request copies be provided electronically, and then print and file a single hard copy. If additional information is provided in hard copy, the IO should ensure that it is scanned and named appropriately, as set out in paragraph 13.8.

13.12 IOs must also take care to ensure that once information is filed, it is immediately deleted from their email and scanning folders.

13.8 Unless the case involves national security or is deemed exceptionally sensitive by HOE (when separate arrangements will be made), the paper files and document boxes will be kept in a locked cupboard in the IO’s room. The cupboards must be kept locked at all times, except when in use.

13.9 Files and document boxes must never be left unattended and must be locked away when not in use. IOs will be expected to return the file to its cupboard at the end of each day.

13.10 For procedure on taking files out of the building, see 13.29 below.

13.11 At the end of a case (see procedures for timescales and what to do if a case is being appealed), all documentary evidence submitted to OSIC will be destroyed, unless the party – usually the public authority – which provided it requires it to be returned. The contents of the paper file will be destroyed. OSIC is a green office and the paper file and document box must be returned to Admin for re-use.

13.12 An exception is made for cases which SIC has identified as important to retain within OSIC for a longer period – see Appendix 9.

Original evidence – register

13.13 The receipt and return of all original evidence (not copies) received from public authorities or applicants will be logged.

13.14 A register for this purpose will be maintained in the form of a notebook kept with the mail book, which will record:

- the evidence owner (name of public authority)
- file number (if applicable)
- file titles
- general document descriptions (e.g. “correspondence”, “accounts”)
- date and time of receipt (and return)
- name of staff member responsible for the evidence.

13.15 This register will be completed at the point of receipt (i.e. by staff opening the post) and also on return of the original evidence.

13.16 Staff responsible for completing the original evidence register must also alert the VO, who will add a note to the case file in WorkPro.

Handling original evidence

13.17 OSIC tries to avoid accepting originals of evidence wherever possible. Officers should try to explore all other reasonable options before requesting or accepting originals. Only rarely should officers agree to go to public authorities to copy or view documents and then only with the prior approval of the HOE or DHOE.

13.18 If originals of evidence are accepted, a schedule of items being sent must also be requested. This must be checked at the point of receipt by the officer or responsible team member if the IO is not available to ensure that it tallies with the information sent.

13.19 If this schedule is not received, or is not accurate, the owning authority must be contacted to confirm what has been received by us.

13.20 On receipt of original evidence, a letter or e-mail must be sent to the public authority detailing what has been received. This should also tell the authority that the evidence will not be returned until three months after the decision notice is issued or (where no decision is required) the case is closed.

13.21 Any schedule received must be scanned separately by Admin and saved in the WorkPro file.

13.22 A note must be made in WorkPro by the officer to show that originals have been received. (In most cases this will simply take the form of the schedule that has been enclosed with the original evidence.)

13.23 Any original evidence received must be kept in the secure store.

13.24 Whilst original evidence is with OSIC, it is the responsibility of the officer to ensure that it is kept safely and is not lost. If the evidence is passed to another member of staff (e.g. when a draft decision is given to the HOE or DHOE for approval), a note must be made in WorkPro to record this fact.

13.25 Original evidence must *never* be removed from the building, except when meeting the owning authority to discuss the case involved. If this is done, the checking out procedure for files must be followed (see **Removing OSIC Files from the Building** below).

13.26 Any notes on pages of original evidence must be made lightly in pencil or, preferably, on post-it notes. Notes must never be made on original evidence in pen.

13.27 At the end of the investigation, original evidence must be sent back to the owning authority, either by hand, by recorded delivery or by courier. The officer should enclose a covering letter detailing what is being returned, and requesting confirmation of receipt. The evidence must be securely packaged to prevent any unauthorised access and damage from the elements. If there is any uncertainty over who to send the information to, officers must contact the owning authority to find out the most appropriate person/department to send it to.

13.28 Once the originals leave the building, the officer must make a note of this in WorkPro, as well as in the Original Evidence register in Bell.

Removing case files from the building

13.29 Ideally case files should not be taken out of the office, but if there is a genuine need to do this, it must be cleared with HOE, DHOE, or HOOM first.

13.30 A record of this permission, stating the period that the file has been allowed out for, must be logged in the outgoing file register, held by HOE, at the point of removal. Return of the file must also be recorded in the register.

File security when outside the building

13.31 In the rare event of files being taken out of the building, it is the officer's responsibility to ensure that the files are not put at risk. The following guidance should be followed by staff:

- Files must be returned to the office as soon as possible. Files should be taken straight home, or straight to the meeting with the public authority involved. If this is not possible, they must be locked out of sight in the boot of the car only until such time they can be returned to the office or, failing which, kept temporarily in the officer's home.
- When carrying files in public, officers must ensure that they are concealed and well protected from the elements. Never leave files unattended in public.
- Officers must not work with files on public transport or in public areas, e.g. cafés. They may contain exempt information and so should not be put at risk of being accessed by the general public. This is applies especially to original evidence files being taken to a meeting with a public authority.

Procedure for lost or stolen files

13.32 In the event of a file going missing whilst it is out of the building:

- If it is lost, the responsible officer must check all places where it might have been left/stored.

- If it cannot be found after extensive searching, the officer must inform HOE, DHOE or HOOM immediately, who will then assess whether the file is at risk of unauthorised access, what information has been lost and what information is recoverable from scanned versions.
- If the file has been stolen HOE, DHOE or HOOM must be informed immediately and will inform the local police in the area where it was stolen, if they have not been informed already. Again, they should also determine with the member of staff what information has been lost and what is recoverable from scanned documents.
- If an original evidence file has been lost in transit every effort must be made to locate it. If this fails, the responsible Officer must then inform HOE, DHOE or HOOM, who will contact the public authority to inform it, and determine if the police should be informed.
- If an original file has been stolen in transit, HOE, DHOE or HOOM should be informed and will contact the police in the area where it was stolen, if they have not already been informed.
- It is the responsibility of the HOE to inform the public authority, as soon as possible, that the information has been lost or stolen.

Procedure for dealing with withheld information at case closure

13.33 When the VO/IO destroys the paper file and closes the case, any withheld information will also be deleted from the WorkPro file. Information will only be returned to the authority where it has been provided in paper form and its return has specifically been requested. The VO/IO will note in the WorkPro file that the information has been destroyed or returned, as appropriate. (Until the previous case handling system, CHAS, has been fully closed down, it will also be necessary to ensure that any withheld information is also destroyed from the CHAS file.)

8.6 - Certificate of Destruction – IT

Certificate No. R12/03/122

RESTRUCTA

Certificate of Secure Destruction

Shipped From: Scottish Information Commission (DoC: 3649)

Product Description: Redundant IT Equipment

Destruction Method Used:

- Dismantling of equipment for disposition into appropriate waste streams.
- Circuit boards granulated for precious metal refining.
- Hard drives shredded and melted for scrap metal.
- All ferrous metal casings and housings recycled as scrap metal.
- Recycling of any re-usable plastics from housing and assemblies.

Carried Out By: Restructa Limited, 15-16 Arkwright Way, North Newmoor Ind Est, Irvine, KA11 4JU

Witnessed By: [redacted] **Date:** 30/3/12

(Process Manager)

ISO 14001 REGISTERED FIRM

ISO 9001 REGISTERED FIRM

Approved Authorised Treatment Facility – WEE/SE0722PA/ATF
Waste Management Licence – WML/W/220288, Waste Carriers Licence – SCO/046355

Element 9 – Data Protection

9.1 - Employee handbook (extract) – Section 12.3

Section 12.3 - Data Protection Policy in relation to Employee Information

Data Protection Principles

182. As an employer, the Commissioner recognises the importance of safeguarding personal privacy when dealing with information about its staff. The Data Protection Act 1998 (DPA) requires us to inform you what data we hold on you and the purposes for which this data might be used. Additionally, the DPA requires us to process your personal data[1] in accordance with the following data protection principles:

- Personal data will be processed[2] fairly and lawfully.
- Personal data will be obtained only for specified and lawful purposes, and will not be processed further in any manner incompatible with those purposes.
- Personal data will be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- Personal data will be accurate and, where necessary, kept up to date.
- personal data shall not be kept for longer than is necessary for the purposes for which it is obtained.
- Personal data shall be processed in accordance with the rights of individuals.
- appropriate measures will be taken against unauthorised or unlawful processing of personal data and against its accidental loss, damage or destruction.
- Personal data shall not be transferred to a country outside the European Economic Area without the consent of the data subject unless that country or the transferee is deemed to ensure an adequate level of protection for the processing of personal data and the rights and freedoms of data subjects.

Why do we hold personal data about workers?

183. We collect, maintain and process personal data about employees to enable us to conduct our business, in particular our payroll and personnel functions. We also process personal data to enable us to comply with legal and tax requirements.

To whom might we disclose personal data?

184. We supply personal data to:

[1] Personal data means any information which relates to you and allows you as an individual to be identified.

[2] **Processing** means obtaining, recording or holding information or data or carrying out any other operation on the information or data. This includes the organisation, adaptation, alteration, retrieval, consultation, use, disclosure or otherwise making available, alignment, combination, blocking, erasure or destruction of the information or data.

- individuals who are legally entitled to the information
- those who provide us with electronic data processing services, technical initiatives of benefit to the Commissioner, or other professional or management services such as payroll administration, insurance, health or legal services
- any authority to which we are required by law to disclose personal data (for example, the Inland Revenue, the Health and Safety Executive etc)
- anyone to whom we are otherwise required to disclose it, such as employees seeking access to their own personal data.

Publication on the Internet

185. Generally, the only personal data which would be on the Commissioner's internet website is the name, job title, function and photograph of staff. This limited information is to enable the public to access appropriate staff in accordance with the policy to be open and accessible.

Sensitive personal data

186. Certain information about you is regarded as "sensitive personal data" under DPA. We can only process such data under strict conditions. Sensitive personal data may only be processed if:

- the individual has given explicit consent to the processing of the data or
- one of the other conditions set out in DPA applies to the processing.

187. Sensitive personal data includes any data revealing:

- your racial or ethnic origins
- your political opinions
- your religious beliefs or other beliefs of a similar nature
- your membership or otherwise of a trade union
- your sexual life
- your physical or mental health or condition
- the commission or alleged commission by you of any offence or
- any proceedings or sentence imposed for any offence committed or alleged to have been committed by you.

188. It is the Commissioner's policy at all times to keep any sensitive personal data we hold and process to a minimum. Unless we are permitted to do otherwise under DPA, we will also obtain your explicit consent before such data is processed. We may require to process sensitive personal data for the following purposes:

- in relation to your physical or mental health or condition, for the purpose of sickness records we are required to maintain relevant to your employment
- for equal opportunities monitoring and
- for any other purpose that is necessary to allow us to comply with our statutory obligations.

189. If we wish to carry out any additional processing which is not otherwise permitted under DPA and specifically by conditions in Schedules 2 and 3, we will first obtain your explicit consent to the processing.

Security of personal data

190. The Commissioner will ensure that adequate technical and organisational security measures are taken so that privacy is preserved whenever and wherever processing of personal data (including sensitive personal data) takes place. This is achieved by observance and regular review of our existing Security and IT Security Policies.

Access to personal data

191. All staff are entitled to reasonable access to their own personal data to verify it and put right any inaccuracies. The Commissioner aims to achieve an annual issue of data to all staff for the purposes of updating and correction. If you wish to access your personal data at other times, you should submit a written application (commonly referred to as a "subject access request") to the HOOM describing the information that you seek. We will then process your subject access request in accordance with DPA. Please note that there are certain types of information that are exempt from this general right of subject access and which we may not disclose to you.

Updating personal data

192. We wish to ensure that personal data is kept accurate and up to date. If you feel that your personal data may be inaccurate please contact the FAM to discuss the matter further.

Updating the policy

193. This policy may be updated from time to time to take account of changes in technology and to reflect our legal obligations.

Misuse of employee data

194. It is an offence under DPA for employees to disclose the personal data of others to third parties or procure the disclosing of such personal data to third parties without the consent of the Commissioner. Any misuse of personal data by employees will be treated extremely seriously and may constitute a disciplinary offence under the disciplinary procedure. If you are concerned about a request to disclose any employee information please contact the HOOM.

Freedom of Information

195. As a Public Authority, the Commissioner is subject to requests from private individuals under FOISA or the EIRs. The Commissioner has a duty to provide information in response to requests made under FOISA or the EIRs subject to the exemptions, etc. contained in the legislation.

196. Amongst other things, such requests may call for the disclosure of personal data about staff. The Commissioner will apply the principles of DPA to each request and the level of

disclosure will be decided on its merits. You should be aware, however, that an internal review under FOISA can overrule an initial decision that information should be withheld.

197. The Commissioner may inform and/or consult staff on certain FOI requests. The circumstances under which staff may be informed or consulted are:

198.

Nature of Information about Employees	Staff informed or consulted
Purely incidental references to names/jobs	No
Specific enquiry about job title of identified/identifiable individuals	No
Nature of Duties (other than arising from purely incidental reference e.g. when a memo happens to disclose type of work)	Yes
Information disclosing actions taken by identified individuals in the course of work in non-controversial circumstances	No
As above but information might be expected to focus further attention on employee	Yes
Enquiries designed to ascertain actions taken by identifiable members of staff	Yes
Pay, allowances and expenses (of identified or identifiable individual rather than grade)	Yes
Any disciplinary matter	Yes
Any information about private life	Yes

199. The criteria suggested here relate only to the circumstances in which the Commissioner may inform and/or consult you about FOI requests. While the Commissioner will take into account your views about whether or not information should be disclosed, she will take decisions on the basis of the circumstances of each individual request and in the light of any relevant case law.

How to obtain further information

200. You have certain statutory rights concerning the provision by us of information regarding the manner in which we store and process your personal data. If you wish to raise an issue relating to your personal data or data protection, please contact the HOOM.

201. The rights that you have under this policy do not affect any rights that you may have under DPA or any other Act, rules or regulation.

9.2 - Enquiries Procedure (extract) – Section 5

Subject Access Requests

What are Subject Access Requests?

Subject access requests (SARs) are requests to OSIC for information about (and identifying) a living person, made by that person. However, in some cases, a SAR may be made by a third party, e.g.

- by a parent on behalf of a young child
- by a representative on behalf of an adult with incapacity
- by a solicitor on behalf of a client.

We must take reasonable steps to make sure that the person making the SAR is who they say they are. If someone is making a request on behalf of a third party, we need to check that they have the authority to make that request.

If they do not, their request should be treated as a request for third party personal information under FOISA or the EIRs. Where this happens, the information is likely to be exempt.

Remember that, from 8 April 2013, any person who has been allocated an information request must issue an Equality Monitoring Form. This should be done when the request is acknowledged. Templates have been set up in WorkPro for this.

Format of SARs

The Data Protection Act 1998 (the DPA) specifies that all SARs must be made in writing. Requests can be made by email, fax etc. Depending on how it is framed, a SAR may also be an information request under FOISA or the EIRs: if it is, it should be refused as such under section 38(1)(a)/regulation 11(1), before going on to respond to the SAR.

Timescales

The DPA states that a data controller (i.e. OSIC) shall comply with a SAR within **40 calendar days** (not working days) of receiving a request from a requester or their representative (see below, under "Processing a subject access request" for when this period starts).

Information to be provided

The requester is entitled to the following information in response to a SAR, in addition to the personal data in question:

- confirmation of whether OSIC is processing (i.e. holds) their personal data

- a description of any personal data held
- the purposes for which the data are being or will be processed
- any recipients or classes of recipients to whom the data are or may be disclosed (basically, any persons or organisations who might receive the data in the course of processing, but not anyone - such as the police or other law enforcement agencies - who might obtain the data in pursuance of a statutory right)
- any information held as to the source of the data
- details of the logic involved in any automated decision-making about the requester (highly unlikely to arise in relation to data held by OSIC).

In relation to the description of the data, the purposes and the recipients, it should be sufficient to refer to general categories rather than being any more specific.

The personal data must be provided in an intelligible form. This must be a permanent form, unless either (a) doing so would involve disproportionate effort, or (b) the requester agrees otherwise: we should approach SARs on the basis that the data will be provided in permanent form. If the personal data contain codes or indicators which can only be understood by reference to a key, or if they contain abbreviations, technical terms or jargon, then these must be explained to the requester.

When considering what information should be provided in response to the SAR, bear in mind that what the applicant is entitled to is his/her personal data, as defined in section 1(1) of the DPA. This will not necessarily mean everything OSIC holds relating to an application/enquiry the requester has made.

In areas of doubt, consult the relevant guidance produced by the ICO[3], particularly "Determining what is personal data" http://www.ico.gov.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Detailed_specialist_guides/PERSONAL_DATA_FLOWCHART_V1_WITH_PREFACE001.ashx and "Access to information held in complaint files" http://www.ico.gov.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Practical_application/access_to_information_held_in_complaint_files.ashx: any remaining questions should be discussed with the HOE/DHOE.

As with information requested under section 1 of FOISA, reasonable care should be taken to secure any information covered by a SAR against destruction between the time the request is received and the time it is responded to.

Non-specific requests

In some cases, OSIC may not have sufficient information to allow it to confirm the requester's identity or locate the information the requester is seeking. If the requester is asked for that information but fails to provide it, OSIC does not have to comply with the request.

---

3 http://www.ico.gov.uk/for_organisations/guidance_index/data_protection_and_privacy_and_electronic_communications.aspx

Similar or repeated requests

OSIC does not need to comply with a SAR if it has already complied with an identical or similar request by the same individual, unless a reasonable interval has passed between compliance with the previous request and the making of the current request. In deciding what amounts to a reasonable interval, consideration must be given to the nature of the data, the purposes for which OSIC processes the data and the frequency with which the data are altered.

Charging

We can charge up to £10 for complying with a SAR. It is our policy not to charge.

There are specific provisions providing for access to "unstructured personal data". If the data requested fall into this category, we are under no obligation to comply with the request where the cost of doing so exceeds £450. However, this issue is unlikely to arise in practice: basically, "unstructured personal data" are manual records. Consequently, we are likely to hold information in that form only where it is of exceptional sensitivity, in which case it is likely to be exempt from disclosure: any cases which appear to involve unstructured personal data should be discussed with the HOE/DHOE.

Third party information

In some cases, it will be impossible to comply with a SAR without disclosing information relating to another individual who can be identified from that information. It will be possible to identify another individual where they can be identified simply from the information disclosed, or from that information and any other information the data controller considers it reasonably likely is (or will be) in the requester's possession: areas of doubt should be discussed with the HOE/DHOE.

Where compliance would involve disclosure of information relating to and identifying another individual, the request does not have to be complied with unless either (a) the other individual has consented to disclosure of the information or (b) it is reasonable in all the circumstances to disclose the information without that consent. In considering what is reasonable, relevant factors include:

- whether there is any duty of confidentiality owed to the other individual
- any steps taken to seek the other individual's consent
- whether the individual was capable of giving consent
- whether the other individual has expressly refused consent

These must be taken into consideration (and other factors may be relevant, depending on the circumstances), but none of them necessarily preclude disclosure.

It may be possible to separate the information about the other individual from the requester's own personal data, e.g. by redaction of names or other identifiers: if so, this should be done to allow the SAR to be complied with. In such cases, it should also be possible to deal with that part of the

request relating to the other individual's personal data as a separate request under s1 of FOISA (or, where appropriate, the EIRs).

Disclosing third party personal data without a valid reason may be a breach of Article 8 of the European Convention of Human Rights.

Exemptions

In certain limited circumstances, OSIC can refuse to comply with a SAR, either in full or in part. Part IV and Schedule 7 of the DPA set out the exemptions which may be used to withhold information from data subjects. There are exemptions relating to national security and to information processed (not necessarily by OSIC) for various purposes connected with crime prevention and other regulatory functions.

Information subject to legal professional privilege is also exempt, as is information from confidential employment references given by OSIC (or an OSIC employee, acting in that capacity) in relation to the data subject.

OSIC staff should note that it is the policy of OSIC to be as open as possible, in relation to requests under the DPA as well as those made under FOISA or the EIRs. As the DPA derives from a Community obligation, disclosure in response to a SAR will usually be with lawful authority for the purposes of section 45 of FOISA. However, there may be cases where the information relates to matters falling outwith the scope of Community law (in particular, public security, defence, state security [including the state's economic well-being] and criminal law), in which case there cannot be a Community obligation and section 45 may apply. Any case where this appears likely to arise should be discussed with the HOE/DHOE. (See section 4 above on section 45 generally.)

Processing a subject access request

a) Receipt

The request must be in writing. **Remember that the request does not have to mention the Data Protection Act**. The requester might just ask for access to personal data/information/files/records relating to them.

On receipt of the SAR, the HOE or DHOE must be advised that it has been received. The HOE or DHOE will give advice on processing the SAR.

b) Process the Request

The officer, in conjunction with the HOE/DHOE, will check the request to ensure that all of the necessary information has been provided to allow the identification of the requester and the location of the personal data.

If all the necessary information is there, the officer will issue letter **Enq1**.

Where further information is required (such as proof of identity or more details about the information requested), the officer will issue letter **Enq2**.

c) Verify the Identity of the Requester

It is important that the officer is satisfied as to the identity of the requester. Disclosure to the wrong person is likely to have serious consequences, so proof of identity must always be obtained, even where there has been previous contact with the requester. (Requesters should be asked to provide a copy of their passport, driving licence or utility bill.)

Where a third party has made a subject access request on behalf of another person, it is important (in addition to verifying the requester's identity, as required) to check that they have the authority to do so. Use style letter **Enq4**.

d) Start the 40 day count

The **40** day period starts when OSIC has received enough information to identify the requester and to locate the requested data.

e) Contact OSIC Employees

The officer will contact all of the employees in OSIC who are likely to hold the requester's personal data and request a full copy of any data held about the data subject.

f) Collate/consider the information

The officer will collate the information gathered from OSIC staff and consider whether there are genuine reasons for withholding any of it from the requester. This should be discussed with the HOE/DHOE, as appropriate.

g) Respond to the Subject Access Request

Once collated (and redacted, as appropriate), the personal data will usually be sent to the applicant by post. Depending on the sensitivity of the information, it may have to be sent out by recorded delivery. Use style letter **Enq3**. If the information is particularly voluminous, it may be appropriate to ask the requester whether they wish to come to the office and look over the information.

The requester should be provided with a contact or reference point should they wish to discuss any of the information provided in response to their SAR. This will generally, but not always, be the officer who dealt with the SAR.

Appeals and complaints about the procedures

If an individual is unhappy with the response given to their SAR, the matter should firstly be referred to the Scottish Information Commissioner for further consideration, although the requester does not have to accept this route and may go straight to the UK Information Commissioner in Wilmslow.

If the individual is unhappy with the way in which his/her request was handled (i.e. the service they have received, rather than the outcome of the request), you can suggest they make use of the OSIC complaints procedures.

Element 10 – Business Continuity and Vital Record

10.1 - Business Continuity Plan (extract)

Contents

1. Day 1 - 6 action plan

Day 1 - Initial response

	Actions	Responsibility	Ref. page
1	• Initial Response Team (IRT) (SIC & HoDs) meet to assess extent of disaster		
2	• Decision to implement BCP – Scenario 0	• SIC	
3	• Staff informed and Core Recovery Team (CRT) established	• HoDs	4
4	• Temporary base established for IRT	• FAM	8
5	• Emergency Accommodation activated – [redacted] • Microsys instructed to implement recovery plan • SPCB informed • MDDC informed • Insurance Brokers / Insurers informed	• HOOM • HOOM • SIC • SIC/HOOM • HOOM	10 5 & 19 5 5 5 &14
6	• IT recovery plan implemented	• HOOM	19
7	• Email plan implemented	• Administrator	23
8	• Communications plan implemented	• HOPI	26
9	• Enforcement work plan implemented	• HOE	29
10	• Phone plan implemented	• Administrator	30
11	• Postal mail plan implemented	• Administrator	33
12	• Banking plan implemented	• FAM	36
13	• Advance party to set up accommodation at [redacted]	• FAM	10
14	• Day 2 plan reviewed and next steps established	• SIC / HoDs	

Day 2 – Progressing recovery / Interim plans

	Actions	Responsibility	Ref. page
	CRT locate at [redacted]		
1	• IT recovery progressed	• HOOM	18
2	• Enforcement work plan implemented	• HOE	29
3	• Communication Plans continue	• HOPI	26
4	• Day 3 plan reviewed & next steps established	• SIC / HoDs	

Day 3 – Systems recovery achieved

	Actions	Responsibility	Ref. page
	CRT located at [redacted]		
1	• IT recovery completed – full systems access available	• HOOM	18
2	• Enforcement work plan implemented	• HOE	29
3	• Communication Plans continue	• HOPI	26
4	• Arrangements for return to work of remaining staff established	• HoDs	

Day 4 – 6 onwards (as soon as practicable) – full service resumed

	Actions	Responsibility	Ref. page
	Whole staff located at [redacted]		
1	• Recovery of Enforcement Team service	• HOE	
2	• Recovery of P&I service	• HOPI	
3	• Recovery of OMT service	• HOOM	
4	• Establish timescale for return to Kinburn Castle	• HOOM	
5	• Decide if medium term accommodation will be necessary	• SIC / HoDs	
6	• Arrange medium term accommodation if necessary	• HOOM	

[4] Some members of CRT may remain located in temporary accommodation in St Andrews, depending on impact / nature of disaster at Kinburn Castle

2. Core Recovery Team - roles and responsibilities

Role	Key Responsibilities
SIC	• Determining extent of disaster - decision to implement BCP • Take key decisions • Communication with media, SPCB
HOOM	• Determining extent of disaster – decision to implement BCP • Lead responsibility for BCP implementation • Relocation/ IT / Insurance / SPCB • Recovery of full service provision • Interim relocation plans
FAM	• Finance • Banking • Supporting HOOM
Administrators (2)	• Main interaction with Microsys – IT system recovery • Relocation • Supporting implementation of interim relocation plans • Practicalities
HOPI	• Determining extent of disaster – decision to implement BCP • Implementation of communication plan • Identifying and responding to key P&I issues
FOIO (P&I) (1)	• Support HOPI to deal with media and general enquiries • Support HOPI to identify and respond to key issues
HOE	• Determining extent of disaster – decision to implement BCP Maintenance of key cases e.g. active Appeals to the Court of Session • Identifying critical applications requiring immediate attention • Ensuring new applications are safely received and recorded • Dealing with general enquiries
DHOE	• Support HOE to deal with general and case specific enquiries

Element 11 – Audit Trail

11.1 - INVU Destruction Log (extract) - Part 1 of Excel Spreadsheet entry

Date destroyed	Document ID	Revision	Organisation	Description	Subject	Type	Document Author	Checked in	Entry date	Status
Text redacted										

INVU Destruction Log (extract) - Part 2 of Excel Spreadsheet entry

Text redacted

11.2 - Paper Destruction Register (extract)

Date destroyed	No of items	Item Details	Date due for destruction	1st Reviewed by (name)	2nd Reviewed - Approved by (name)	Date Approved	Reason for Destruction	Method of Destruction
Text redacted								

Element 12 – Competency Framework for Records Management Staff

12.1 - Head of Operational Management Job Description (extract)

Reporting to: Scottish Information Commissioner

Strategic Responsibility

To ensure that the SIC operationally is effective, highly responsive and appropriately resourced.

Key functions:

- Develop systems for information and knowledge management (including technical infrastructure, case management and records management systems.)

Element 13 – Review and Assessment

13.1 – Operational Plan 2013/14 (extract)

Information management

	Activity (Activities run for whole year unless stated otherwise)	Type	Frequency	Start Date	End Date	Strategic Aim					Priority
						1	2	3	4	5	
1	Establish (SIC) Publication Scheme Working Group & work programme	Project		01/05/2013	31/01/2014			X		X	H
2	Achieve a "good" rating for the Commissioner's publication scheme	Project		01/06/2013	31/12/2013		X			X	H
3	Case Management System upgrade	Project		01/04/2013	30/06/2013	X		X		X	H
4	Data Protection Officer - review role, train and implement procedures	Project		01/08/2013	31/12/2013					X	H
5	Conduct ARMS assessment of Records Management	Project		01/10/2013	31/12/2013					X	M
6	Prepare and submit a Records Management Plan to the Keeper of the Records for Scotland, to comply with requirements of Public Records (Scotland) Act 2011	Project		01/07/2013	31/01/2014					X	H
7	Conclude 12/13 phase of Records Management Project	Project		01/04/2013	30/06/2013					X	H
8	Implement on-going RM controls and procedures Assurance report to SMT	BAU	Annual	01/07/2013	31/03/2014					X	H
9	Maintenance of secure and reliable IT system	BAU								X	H
10	Create policy and guidance for review of policies, procedures and key documents, including instructions for document control and production of comprehensive register of key documents	Project		01/04/2013	30/06/2013					X	H

	Activity (Activities run for whole year unless stated otherwise)	Type	Frequency	Start Date	End Date	Strategic Aim					Priority
						1	2	3	4	5	
11	Manage policy and procedure, and key documents as per review programme	BAU	Quarterly	01/06/2013	31/03/2014					X	H
12	Deal with information requests and reviews in line with policy and procedure, within statutory time scales	BAU						X		X	H
13	Approve and implement findings of review of information requests process	Project		01/04/2013	30/06/2013			X		X	H

Appendix 1 - Document Control Sheet

Document Information	
Full name of current version: Class, Title, Version No, INVU version no and status. *E.g. C1MOU Between the SIC and the ICv01.25*	Class 5 Scottish Information Commissioner Records Management Plan Evidence Extracts v00.02 (Draft)
INVU No.	INV48284
Type	
Approval	
Approver *(SMT, HOE,HOOM,HOPI)*	SMT
Approval Date	27/01/14
For publication *(Y/N)*	Y
Review	
Responsible Manager (*SIC, HOE, HOOM,HOPI)*	HOOM
Date last major review	31/01/14
Date of last minor review	NA
Date of next regular review	NA
Publication	
Date published	14/07/2014
Date guide to information updated	14/07/2014
Action by *(initials)*	KB
Associated Documents	
Full name(s)	Scottish Information Commissioner Records Management Plan
INVU Number(s)	INV43505
Notes/ comments	**(for the comments column on Register)**

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 HOOM, reviewed whole section on PI test, whole document updated, corrected typos, reformatted to new branding*)
14/07/14	KB	00.01	00.02	DCS updated
14/07/14	KB	00.02	00.02	Uploaded to Guide to Information