

Scottish Information Commissioner

Records Management Plan



Scottish Information
Commissioner

Contents

Glossary and abbreviations.....	i
Covering Statement.....	ii
Element 1: Senior Management Responsibility	1
Element 2: Records Manager Responsibility	2
Element 3: Records Management Policy Statement.....	3
Element 4: Business Classification.....	5
Element 5: Retention Schedules	6
Element 6: Destruction Arrangements.....	8
Element 7: Archiving and Transfer Arrangements	10
Element 8: Information Security.....	12
Element 9: Data Protection	15
Element 10: Business Continuity and Vital Records	19
Element 11: Audit Trail and version control.....	21
Element 12: Records management training for staff.....	24
Element 13: Assessment and review	26
Element 14: Shared Information.....	28
Element 15: Public Records created or held by third parties	32
Appendix 1 – Evidence Schedule.....	33
Document control sheet.....	37

Glossary and abbreviations [to be completed when approved]

Term used	Explanation
PSRA	Public Records (Scotland) Act 2011
The Keeper	Keeper of the Records of Scotland
RM Plan	Records Management Plan
SMT	Senior Management Team
Commissioner	Scottish Information Commissioner
DPA/GDPR	Data Protection legislation
HOCS	Head of Corporate Services
DPO	Data Protection Officer
SPCB	Scottish Parliamentary Corporate Body
DHOE	Deputy Head of Enforcement
DPIA	Data Protection Impact Assessment
FAM	Finance and Administration Manager

Covering Statement

This Records Management Plan (RM Plan) has been put in place to meet the requirements of the Public Records (Scotland) Act 2011 (PRSA).

The PSRA came into force on the 1 January 2013, and requires The Scottish Information Commissioner (the Commissioner) to submit a RM Plan to be agreed by the Keeper of the Records of Scotland (the Keeper). This document will replace the RM Plan agreed by the Keeper in 2014 and was submitted to the Keeper on 30 June 2021.

I recognise the value of our records as a corporate asset and records management as a key corporate function. Our records are our corporate memory providing evidence of actions and decisions and supporting our daily functions and operations.

Information and records management underpins all that the Commissioner's office does and is part of our annual operational planning. An annual assurance report on records management is a mandatory reporting requirement under our Governance Arrangements and is provided by the Head of Corporate Services who has operational responsibility for records management.

I am committed to ensuring that:

- our policies, procedures and practices are implemented and that they are effective
- we routinely review and develop as necessary our policies, procedures and practices
- all staff maintain, and develop as necessary, their competence in information and records management
- all employees, contractors, agents, consultants and other third parties who have access to any information held within the Commissioner's office, are fully aware of and abide by their information and records management duties under the PRSA.

I also recognise that there is always scope to improve and develop what we do and how we do it. I am committed to continuous improvement and to ensuring that our key documents are actively reviewed, including those relating to information and records management and our processes and procedures.

This RM Plan identifies future developments which, once in place, will further enable us to deliver improvements in records management and business efficiency, helping us to carry out our statutory functions and to comply with legislative requirements.



Daren Fitzhenry
Scottish Information Commissioner
30 June 2021

Element 1: Senior Management Responsibility

Introduction	<p>A compulsory element of the Public Records (Scotland) Act 2011.</p> <p>This element must identify the person at senior level who has corporate responsibility for records management within the organisation.</p>
Statement of Compliance	<p>The senior person who has overall corporate responsibility for records management is Daren Fitzhenry, the Scottish Information Commissioner.</p>
Evidence of Compliance	<p>Evidence submitted in support of Element 1 comprises:</p> <ul style="list-style-type: none">• The Covering Statement which forms part of this document• Information and Records Management Policy
Future Developments	<p>There are no planned future developments in respect of Element 1.</p>

Element 2: Records Manager Responsibility

Introduction	<p>A compulsory element of the Public Records (Scotland) Act 2011.</p> <p>An individual staff member is identified as holding operational responsibility for records management and has appropriate corporate responsibility, access to resources and skills.</p>
Statement of Compliance	<p>The senior manager with operational responsibility for records management is Helen Gardner-Swift, Head of Corporate Services</p>
Evidence of Compliance	<p>Evidence submitted in support of Element 2 comprises:</p> <ul style="list-style-type: none">• The Covering Statement which forms part of this document• Information and Records Management Policy• Information and Records Management Handbook
Future Developments	<p>There are no planned future developments in respect of Element 2.</p>

Element 3: Records Management Policy Statement

<p>Introduction</p>	<p>A compulsory element of the Public Records (Scotland) Act 2011.</p> <p>This element must describe how the organisation creates and manages authentic, reliable and usable records, capable of supporting business functions and activities for as long as they are required.</p>
<p>Statement of Compliance</p>	<p>The Scottish Information Commissioner recognises the value of our records as a corporate asset, and records management as a key corporate function.</p> <p>Our commitment and overall approach are set out in the Information and Records Management Policy.</p>
<p>Evidence of Compliance</p>	<p>Evidence submitted in support of Element 3 comprises:</p> <ul style="list-style-type: none"> • Information and Records Management Policy
<p>Future Developments</p>	<p>The Information and Records Management Policy will be reviewed on an annual basis.</p> <p>COVID –19 pandemic</p> <p>As a result of the impact of the COVID-19 pandemic, the following actions have been taken:</p> <ul style="list-style-type: none"> • the office premises have been closed temporarily since 23 March 2020 and remain closed • office security and IT security measures are in place whilst the office premises are temporarily closed • all members of staff are working remotely (with remote access to the office systems) using laptops and mobile phones provided by us and this includes the Commissioner and all members of the Senior Management Team (SMT) • the Retention Schedule has been complied with as far as possible as regards paper records • updated guidance has been issued to staff working remotely covering: <ul style="list-style-type: none"> ○ security of information, including data protection ○ records management - staff working remotely must comply with our information and records management procedures including ensuring that our records are trustworthy, complete, accessible, legally admissible in court and robust ○ data incident procedures ○ how to use Microsoft Teams and guidance on use

	<p>When the office premises are able to re-open, it is likely that blended/hybrid working will be in place and the guidance issued to staff and any relevant policies and procedures will be updated to take account of the revised arrangements (as necessary). There may also be changes to the Information and Records Management Policy and Information and Records Management Handbook.</p>
--	--

Element 4: Business Classification

Introduction	Records are known and are identified within a structure, ideally founded on function.
Statement of Compliance	<p>The Scottish Information Commissioner maintains a File Plan (Business Classification Scheme) which provides a framework for a consistent approach to classifying all records across the organisation regardless of format or records storage location.</p> <p>The File Plan, in conjunction with the Retention Schedule, is used to identify and retrieve records relating to the same function and activity anywhere in the organisation, irrespective of which department produces or receives them.</p> <p>The File Plan is structured in a three-tier hierarchy representing business functions, activities and sub-activities carried out within the function.</p>
Evidence of Compliance	<p>Evidence submitted in support of Element 4 comprises:</p> <ul style="list-style-type: none">• File Plan and Retention Schedule
Future Developments	<p>The File Plan and Retention Schedule are currently under review and being updated and this is project included within the Operational Plan 2021-22. A copy of the revised and approved File Plan and Retention Schedule will be sent to the Keeper.</p>

Element 5: Retention Schedules

<p>Introduction</p>	<p>The Public Records (Scotland) Act 2011 requires a RM Plan to include provision about the archiving and destruction or other disposal of an authority's public records.</p> <p>The procedures should incorporate retention schedules and should detail the procedures that the authority follows to ensure records are routinely assigned disposal dates, that they are subsequently destroyed by a secure mechanism at the appropriate time, or preserved permanently by transfer to an appropriate physical repository or digital preservation system.</p> <p>The principal reasons for creating retention schedules are:</p> <ul style="list-style-type: none"> • to ensure records are kept for as long as they are needed and then disposed of appropriately • to ensure all legitimate considerations and future uses are considered in reaching the final decision. • to provide clarity as to which records are still held by an authority and which have been deliberately destroyed.
<p>Statement of Compliance</p>	<p>The Scottish Information Commissioner maintains a Retention Schedule which:</p> <ul style="list-style-type: none"> • promotes control over the organisation's records; • protects vital information, which the organisation needs in order to function effectively; • provides clear guidance on the retention and disposal of specific and general categories of information; • enables the confident disposal of records which are no longer needed; • ensures information which is subject to Freedom of Information legislation will be available when required; • ensures information which is subject to Data Protection legislation is managed and held in accordance with that legislation • ensures the organisation is not maintaining and storing information unnecessarily; • ensures the retention of the minimum volume of records consistent with economy and efficiency and effectiveness. <p>The retention periods are determined by legal, statutory and business requirements.</p> <p>The Retention Schedule ensures that the same types of records should be managed consistently no matter where the record is held, or who created it.</p>
<p>Evidence of Compliance</p>	<p>Evidence submitted in support of Element 5 comprises:</p> <ul style="list-style-type: none"> • Information and Records Management Policy • Information and Records Management Handbook • Records Review Procedures

	<ul style="list-style-type: none"> • File Plan and Retention Schedule
<p>Future Developments</p>	<p>The project to revise the retention periods was put on hold pending preparations for DPA 2018 and (EU) GDPR implementation. This project restarted in 2019-20, was partly undertaken in 2020-21 and has now been carried forward into 2021-22. It is hoped that we will be able to create more automated processes and tasks to support the records review processes subject to our duties and responsibilities as regards data protection and personal information.</p> <p>The following documents are currently under review and being updated –</p> <ul style="list-style-type: none"> • Records Review Procedures • File Plan and Retention Schedule <p>A copy of the revised and approved documents will be sent to the Keeper.</p> <p>COVID –19 pandemic</p> <p>As a result of the impact of the COVID-19 pandemic, the following actions have been taken:</p> <ul style="list-style-type: none"> • the office premises have been closed temporarily since 23 March 2020 and remain closed • office security and IT security measures are in place whilst the office premises are temporarily closed • all members of staff are working remotely (with remote access to the office systems) using laptops and mobile phones provided by us and this includes the Commissioner and all members of the SMT • the Retention Schedule has been complied with as far as possible as regards paper records

Element 6: Destruction Arrangements

<p>Introduction</p>	<p>A compulsory element of the Public Records (Scotland) Act 2011 (Section 1(2)(b)(iii))</p> <p>Records are destroyed in a timely and appropriate manner and records of their destruction are maintained.</p>
<p>Statement of Compliance</p>	<p>The Scottish Information Commissioner's Information and Records Management Handbook sets out our approach to the disposal of records.</p> <p>The Records Review Procedures provide detailed guidance on the steps to be taken to dispose of records. These cover the various software packages used by the Commissioner and paper records.</p>
<p>Evidence of Compliance</p>	<p>Evidence submitted in support of Element 6 comprises:</p> <ul style="list-style-type: none"> • Information and Records Management Handbook • Records Review Procedures • Information and Records Management Policy • File Plan and Retention Schedule • Certificate of Destruction – paper records (sample)
<p>Future Developments</p>	<p>The project to revise the retention periods was put on hold pending preparations for DPA 2018 and (EU) GDPR implementation. This project restarted in 2019-20, partly undertaken in 2020-21 has now been carried forward into 2021-22. It is hoped that we will be able to create more automated processes and tasks to support the records review processes subject to our duties and responsibilities as regards data protection and personal information.</p> <p>The following documents are currently under review and being updated –</p> <ul style="list-style-type: none"> • Records Review Procedures • File Plan and Retention Schedule <p>A copy of the revised and approved documents will be sent to the Keeper.</p> <p>COVID –19 pandemic</p> <p>As a result of the impact of the COVID-19 pandemic, the following actions have been taken:</p> <ul style="list-style-type: none"> • the office premises have been closed temporarily since 23 March 2020 and remain closed • office security and IT security measures are in place whilst the office premises are temporarily closed • all members of staff are working remotely (with remote access to the office systems) using laptops and mobile phones provided

	<p>by us and this includes the Commissioner and all members of the SMT</p> <ul style="list-style-type: none">• the Retention Schedule and destructions arrangements have been complied with as far as possible as regards paper records
--	---

Element 7: Archiving and Transfer Arrangements

<p>Introduction</p>	<p>A compulsory element of the Public Records (Scotland) Act 2011 (Section 1(2) (b) (iii)).</p> <p>The RM Plan must detail the archiving and transfer arrangements that are in place and ensure that records of enduring value are deposited in an appropriate archive repository. The details should include the following: how custody of the records will transfer from the operational side of the authority to either an in-house archive, if that facility exists, or another suitable repository, which must be named. The service responsible for the archive should be cited.</p>
<p>Statement of Compliance</p>	<p>There is a Memorandum of Understanding between the Keeper of the Records of Scotland and the Scottish Information Commissioner.</p> <p>This sets out how the process of depositing, storing and accessing records of enduring historical, cultural and research value which have been transferred from the Scottish Information Commissioner to the National Records of Scotland will operate.</p> <p>The MOU identified records which we may wish to transfer in the future. However, there are no immediate plans to transfer as yet, as those records we have identified may still be of operational benefit to us.</p>
<p>Evidence of Compliance</p>	<p>Evidence submitted in support of Element 7 comprises:</p> <ul style="list-style-type: none"> • Memorandum of Understanding between the Keeper and SIC
<p>Future Developments</p>	<p>A revised and updated MOU/Deposit Agreement is being discussed. The Scottish Information Commissioner was established in 2003. To date, no records have been identified which we anticipate it will be appropriate to transfer to the NRS in the future.</p> <p>Internal procedures will be established in conjunction with the Keeper at the appropriate time.</p> <p>Where electronic records are identified for permanent preservation the Commissioner will work with NRS in order to fulfil the requirements of the NRS Deposit Agreement for Electronic Records.</p> <p>The Commissioner will work with the NRS to ensure:</p> <ul style="list-style-type: none"> • the process of transfer ensures the security of the records, that the records are not corrupted in transit (especially in the case of digital records), and the correct records are transferred and received • NRS to confirm that the archives repository has appropriate staff, security and storage to meet the Keeper's requirement • the arrangements for public access to the Commissioner's records is in accordance with access to information legislation and regulation

- | | |
|--|--|
| | <ul style="list-style-type: none">• that access to archive records that include personal data (data relating to living individuals) is in accordance with data protection law. |
|--|--|

Website

There is a project within the Operational Plan 2021-22 to procure a new website (with the intention that this will be designed, built and put in place in 2021-22 and 2022-23. Archiving and transfer arrangements will be considered and taken account of in the specification and design of the new website.

Element 8: Information Security

Introduction	<p>A compulsory element of the Public Records (Scotland) Act 2011, S1(2)(b)(ii).</p> <p>Information security is the process by which an authority protects its records and ensures they remain available. It is the means by which an authority guards against unauthorised access and provides for the integrity of the records.</p> <p>Information security also refers to records in all or any format as all are equally vulnerable. It refers to damage from among other things: computer viruses, malware, flood, fire, vermin, mould, accidental damage, information breach or malicious actions.</p> <p>Information security procedures should normally acknowledge data protection and freedom of information obligations as well as any specific legislation or regulatory framework that may apply to the retention and security of records.</p> <p>Information security procedures should also have in place adequate controls to prevent unauthorised access, destruction, alteration or removal of records and allocate information security responsibilities within the authority to ensure organisational accountability.</p>
Statement of Compliance	<p>The Commissioner recognises that information is a valuable asset and that business continuity is dependent on its integrity and continued availability. Therefore, steps are taken to protect information assets from unauthorised use, modification, disclosure or destruction, whether accidental or intentional.</p> <p>The Commissioner is committed to the secure use of information and information technology systems in order to protect the availability, integrity and confidentiality of the information under our control.</p> <p>The Commissioner also has in place security measures to ensure that physical records are adequately protected. Various improvements arising from a security review which took place in 2015-16 were implemented and security was further reviewed as part of GDPR implementation in 2017-19.</p> <p>The following are in place to protect the information under the Commissioner's control:</p> <ul style="list-style-type: none">• procedures to assess and contain information security risk• information security provision which meets relevant information security compliance requirements• appropriate security measures to protect records involving personal data and ensure compliance with the integrity and confidentiality principle.

	<ul style="list-style-type: none"> • although not required to do so, the Commissioner follows the Scottish Government guidance on cyber security and is participating, as far as possible, in the Public Sector Action Plan as part of the Cyber Resilience Strategy issued by the Scottish Government. Appropriate action is taken in response to early warning notices (Crew Notices) that are sent to us by the Scottish Government's Cyber Resilience Unit. • the Commissioner was re-accredited with Cyber Essentials in December 2020 and re-accredited with Cyber Essentials Plus in March 2021 • when working remotely, all members of staff are still bound by our requirements regarding the security of information and have been advised to comply with the Key document C5 Information and Records Management Handbook • staff who are working remotely are required to adopt the same information security measures that they would take if working in the office premises • access to personal information has also been limited to only those employees, agents, contractors and other third parties who are permitted to access this information • appropriate back-up arrangements, revised to take account of business continuity arrangements, are in place.
<p>Evidence of Compliance</p>	<p>Evidence submitted in support of Element 8 comprises:</p> <ul style="list-style-type: none"> • Information and Records Management Policy • Information and Records Management Handbook • Data Protection Policy and Handbook • Employee Handbook • Investigations Handbook • Risk Register (extract) • Staff Manual (Clear Desk Policy) (extract) • Remote working guidance issued to all staff (extract) • Certificate of Destruction – IT (sample) • Cyber Essentials Certificates – CE and CE+
<p>Future Developments</p>	<p>The information security measures are kept under regular review.</p> <p>COVID –19 pandemic</p> <p>As a result of the impact of the COVID-19 pandemic, the following actions have been taken:</p> <ul style="list-style-type: none"> • the office premises have been closed temporarily since 23 March 2020 and remain closed • office security and IT security measures are in place whilst the office premises are temporarily closed • all members of staff are working remotely (with remote access to the office systems) using laptops and mobile phones provided

by us and this includes the Commissioner and all members of the SMT

- updated guidance has been issued to staff working remotely covering:
 - security of information, including data protection
 - records management - staff working remotely must comply with our information and records management procedures including ensuring that our records are trustworthy, complete, accessible, legally admissible in court and robust
 - data incident procedures
 - how to use Microsoft Teams and guidance on use

When the office premises are able to re-open, it is likely that blended/hybrid working will be in place and the guidance issued to staff and any relevant policies and procedures will be updated to take account of the revised arrangements (as necessary). There may also be changes to the information security measures.

Element 9: Data Protection

<p>Introduction</p>	<p>The Keeper expects an authority’s RM Plan to indicate compliance with its data protection obligations. This might be a high level statement of public responsibility and fair processing.</p> <p>If an authority holds and processes personal data about stakeholders, clients, employees or suppliers, it is legally obliged to protect that information. Under data protection law an authority must only collect information needed for a specific business purpose, it must keep it secure and ensure it remains relevant and up to date.</p> <p>The authority must also only hold as much information as is needed for business, historical or research purposes and only for as long as is set out on an agreed retention schedule. The person who is the subject of the information must be afforded access to it on request, unless an exemption applies.</p>
<p>Statement of Compliance</p>	<p>The Commissioner complies with the data protection obligations.</p> <p>Data protection requirements changed from 25 May 2018 when the EU GDPR and Data Protection Act 2018 came into force.</p> <p>Following an implementation project led by the Head of Corporate Services (HOCS) and assisted by the GDPR Working Party, the Commissioner has in place the appropriate technical and organisational measures to meet data protection and accountability requirements, including the following:</p> <ul style="list-style-type: none"> • a comprehensive data protection policy <ul style="list-style-type: none"> ○ the updated and revised Key Document C5 Data Protection Policy and Handbook was approved in March 2021 and has now been published. ○ all members of staff have been advised that the update and revised document is in place. • a data protection officer (DPO) <ul style="list-style-type: none"> ○ the Scottish Parliamentary Corporate Body (SPCB) has provided a shared DPO service and the MOU for this was signed on 24 May 2018. The MOU is renewed annually. ○ the Commissioner’s DPO is Robin Davidson, Head of Information Governance and DPO, Information Management and Governance Team, The Scottish parliament SPCB, Edinburgh. ○ Euan McCulloch, Deputy Head of Enforcement (DHOE), has agreed to act as DPO if a conflict of interest arises in the operation of the shared service DPO ○ the HOCS is a member of the DPO Networking Group, established by the DPO and, also, meets annually with the

	<p style="text-align: center;">DPO</p> <ul style="list-style-type: none"> ○ the SMT meets annually with the DPO • procedures for the recording and management of data incidents and data breaches • privacy by design guidance, Data Protection Impact Assessment (DPIAs) procedures and templates – DPIAs are carried out where required • data protection impact assessments are carried out. • mandatory annual staff training • revised contracting guidance and model terms and conditions • update of Committee Report templates <p>The Key Document C5 Privacy Notice is in place and is regularly reviewed which enables:</p> <ul style="list-style-type: none"> • the Commissioner to be transparent about the processing of personal data; and • individuals to determine what information the Commissioner holds about them, how it is used, how long it is held and how they can exercise their rights. <p>When working remotely, all members of staff are still bound by our requirements regarding the security of information and are expected to continue to comply with the Information and Records Management Handbook</p> <p>Staff who are working remotely are required to adopt the same information security measures that they would take if working in the office premises</p> <p>Access to personal information is limited to only those employees, agents, contractors and other third parties who are permitted to access this information.</p> <p>Appropriate back-up arrangements, revised to take account of business continuity arrangements are in place.</p>
<p>Evidence of Compliance</p>	<p>Evidence submitted in support of Element 9 comprises:</p> <ul style="list-style-type: none"> • Data protection Policy and Handbook • Privacy Notice • Employee Handbook • Responding to Information Requests: Guidance and Procedures • Additional Temporary Guidance Remote Working (records management (Managing Information remotely) (extract – paragraphs 64-79) <p>The Commissioner’s Registration Reference with the Information Commissioner’s Office is Z8091699</p>

<p>Future Developments</p>	<p>The DPO MOU has been reviewed, the Commissioner has been consulted and provided comments on the revised document and is awaiting details for the signing of the document from the Scottish Parliamentary Corporate Body (SPCB). This work has been delayed (due to the impact of the COVID-19 pandemic) and it is now intended that the MOU will cover 2020-21 and 2021-22.</p> <p>The UK left the EU on 31 January 2020 and the transition period ended on 31 December 2020. As regards relevant terminology, we now operate under the “UK GDPR” with references to the EU’s version being the “EU GDPR”. Our contracts, policies, correspondence and relevant documentation should now refer to “UK GDPR”, where appropriate, to distinguish the difference between these regimes and the work on this is continuing as and when policies, procedures and documentation are reviewed.</p> <p>The Commissioner is also keeping under review:</p> <ul style="list-style-type: none"> • the anticipated adequacy decision to ensure that any required organisational changes are put in place following this decision • the revised the Standard Contractual Clauses (SCCs) for international data transfers and other transfer mechanisms. <p>Simply Personnel - this is a very basic system and information is held securely and access restrictions are in place. However, there is currently no process for the management of the content of the SP database. In 2021-22, we will be procuring a different system which will enable us to manage the content of a database going forward.</p> <p>Work on the retention schedule was delayed in 2020-21 due to the impact of the COVID-19 pandemic this work will now take place in 2021-22 as set out in Element 4.</p> <p>COVID –19 pandemic</p> <p>As a result of the impact of the COVID-19 pandemic, the following actions have been taken:</p> <ul style="list-style-type: none"> • the office premises have been closed temporarily since 23 March 2020 and remain closed • the DPO has been informed of the temporary closure of the office premises and is updated following each SMT review of this decision • office security and IT security measures are in place whilst the office premises are temporarily closed • in accordance with ICO guidance, we are taking a proportionate approach to adapting the way we work and sharing information • all members of staff are working remotely (with remote access to the office systems) using laptops and mobile phones provided by us and this includes the Commissioner and all members of the SMT
-----------------------------------	---

	<ul style="list-style-type: none">• updated guidance has been issued to staff working remotely covering:• security of information, including data protection• records management - staff working remotely must comply with our information and records management procedures including ensuring that our records are trustworthy, complete, accessible, legally admissible in court and robust<ul style="list-style-type: none">○ data incident procedures○ how to use Microsoft Teams and guidance on use <p>When the office premises are able to re-open, it is likely that blended/hybrid working will be in place and the guidance issued to staff and any relevant policies and procedures will be updated to take account of the revised arrangements (as necessary).</p>
--	--

Element 10: Business Continuity and Vital Records

<p>Introduction</p>	<p>Authorities should have appropriate business continuity plans ensuring that the critical business activities referred to in their vital records will be able to continue in the event of a disaster. How each authority does this is for them to determine in light of their business needs, but the plan should point to it.</p>
<p>Statement of Compliance</p>	<p>The Commissioner has a Business Continuity Policy and a Business Continuity Plan which allows the organisation to recover quickly in the event that we experience the loss of access to our office premises for an extended period, as foreseen in those documents.</p> <p>The Commissioner's recognises the importance of the recovery of records in the event of an emergency affecting the office premises or systems. The business continuity arrangements include the following:</p> <ul style="list-style-type: none"> • recovery of records made temporarily unavailable due to an unexpected event • accessing records vital to core business activities and include access arrangements for insurance details, business contract information, key contacts, banking arrangements, personnel files, case files, etc. <p>Arrangements are also in place to ensure the ongoing confidentiality, integrity, availability and resilience of records involving personal data.</p> <p>As the Business Continuity Policy and Business Continuity Plan are key documents, there is a regular review procedure in place which is monitored by the HOCS, the FAM and the SMT.</p> <p>The Commissioner's business continuity arrangements are currently under review.</p>
<p>Evidence of Compliance</p>	<p>Evidence submitted in support of Element 10 comprises:</p> <ul style="list-style-type: none"> • Business Continuity Policy (approved in 2017) • Business Continuity Plan (extract)
<p>Future Developments</p>	<p>The Business Continuity Policy and the Business Continuity Plan are under review.</p> <p>COVID –19 pandemic</p> <p>As a result of the impact of the COVID-19 pandemic, the following actions have been taken:</p> <ul style="list-style-type: none"> • the office premises have been closed temporarily since 23 March 2020 and remain closed • the DPO and other external parties have been informed of the temporary closure of the office premises and are updated

	<p>following each SMT review of this decision</p> <ul style="list-style-type: none">• office security and IT security measures are in place whilst the office premises are temporarily closed• all members of staff are working remotely (with remote access to the office systems) using laptops and mobile phones provided by us and this includes the Commissioner and all members of the SMT• updated guidance has been issued to staff working remotely covering:<ul style="list-style-type: none">○ security of information, including data protection○ records management - staff working remotely must comply with our information and records management procedures including ensuring that our records are trustworthy, complete, accessible, legally admissible in court and robust○ data incident procedures○ how to use Microsoft Teams and guidance on use <p>When the office premises are able to re-open, it is likely that blended/hybrid working will be in place and the guidance issued to staff and any relevant policies and procedures will be updated to take account of the revised arrangements (as necessary). There may also be changes to the Business Continuity Policy and the arrangements in the Business Continuity Plan.</p>
--	--

Element 11: Audit Trail and version control

<p>Introduction</p>	<p>The Keeper expects an authority's records management system to provide evidence that the authority maintains a complete and accurate representation of all changes that occur in relation to a particular record. For the purpose of this plan "changes" can be taken to include movement of a record even if the information content is unaffected. Audit trail information must be kept for at least as long as the record to which it relates.</p>
<p>Statement of Compliance</p>	<p>The Scottish Information Commissioner has systems and procedures in place to ensure an audit trail exists for the editing, movement and destruction of our records.</p> <p>The Commissioner's principal electronic record management systems – Virtual Cabinet (corporate records) and Workpro (casework records) – incorporate full audit trails, incorporating version control (not in Workpro at present but due with next upgrade) and in which the rights to view, edit and delete records are set to reflect organisational policies and procedures.</p> <p>ACT!, a contact management system which holds limited personal data, provides audit trail functionality commensurate with its function as a repository for non – casework related day to day records of communication.</p> <p>Simply Personnel, an HR administration system, maintains a record of changes to, for example, leave records.</p> <p>Paper records</p> <ul style="list-style-type: none"> • A register for non-investigation paper records is maintained and provides guidance on where to store and/or locate paper records • Procedures are in place for the selection and disposal of paper records <p>Workpro</p> <ul style="list-style-type: none"> • Workpro provides a facility to record the staff member who currently has custody and responsibility for a hard copy case file (should a hard copy be required). The location is updated as the case files moves between staff. • Only in exceptional circumstances will case files, or part of case files, be allowed to be taken out of the office or provided for the purposes of remote working • Guidance and procedures are in place and detailed in the Investigations Handbook. <p>Virtual Cabinet Records</p> <ul style="list-style-type: none"> • Version control is built into the software and is initiated when the document is indexed.

	<ul style="list-style-type: none"> • An audit logs of the history of each record is available throughout the life cycle of the record. • The audit log records all actions, movements and amendments and is available to view and print
<p>Evidence of Compliance</p>	<p>Evidence submitted in support of Element 11 comprises:</p> <ul style="list-style-type: none"> • Information & Records Management Policy • Information & Records Management Handbook • Records Review Procedures • Investigations Handbook • DCS example (extract) • Virtual Cabinet destruction log sample (extract) • Paper log sample (extract)
<p>Future Developments</p>	<p>In 2021-22, the following are planned:</p> <ul style="list-style-type: none"> • Review of ACT! • Simply Personnel will be replaced • Workpro upgrade • Virtual Cabinet upgrade <p>COVID –19 pandemic</p> <p>As a result of the impact of the COVID-19 pandemic, the following actions have been taken:</p> <ul style="list-style-type: none"> • the office premises have been closed temporarily since 23 March 2020 and remain closed • the DPO and other external parties have been informed of the temporary closure of the office premises and are updated following each SMT review of this decision • office security and IT security measures are in place whilst the office premises are temporarily closed • all members of staff are working remotely (with remote access to the office systems) using laptops and mobile phones provided by us and this includes the Commissioner and all members of the SMT • updated guidance has been issued to staff working remotely covering: <ul style="list-style-type: none"> ○ security of information, including data protection ○ records management - staff working remotely must comply with our information and records management procedures including ensuring that our records are trustworthy, complete, accessible, legally admissible in court and robust ○ data incident procedures ○ how to use Microsoft Teams and guidance on use <p>When the office premises are able to re-open, it is likely that</p>

	blended/hybrid working will be in place and the guidance issued to staff and any relevant policies and procedures will be updated to take account of the revised arrangements (as necessary).
--	---

Element 12: Records management training for staff

Introduction	<p>The RM Plan must be adhered to by all staff in an authority.</p> <p>The Keeper will expect an authority's RM Plan to detail how the day-to-day operation of activities described in the elements in the authority's RM Plan are explained to the staff who will be required to carry them out.</p> <p>It is important that authorities recognise that records management processes are likely to be implemented by staff in various roles and business areas out-with the immediate information governance officers. These staff members must be trained and supported accordingly. Guidance should be made available.</p> <p>The level of training required by staff will vary considerably depending on their role.</p> <p>Staff processing personal data will require particular training in the handling of those categories of record.</p> <p>It is important that there is a mechanism in an authority that will allow staff to be alerted to changes in records management procedure.</p>
Statement of Compliance	<p>We are a small public authority, with approximately 25 members of staff located in a single office-based premises. Due to the small size of our organisation a dedicated records management post cannot be justified.</p> <p>Records management forms part of the Head of Corporate Services (HOCS) responsibilities. The HOCS is supported by the FAM and the Administrator who have specific records management duties and responsibilities.</p> <p>The Information and Records Management Policy and the Information and Records Management Handbook sets out the competency framework for the HOCS, the FAM and the Administrator.</p> <p>All new members of staff receive induction training on records management and all members of staff receive update training when records management systems are updated, for example, Workpro, Virtual Cabinet.</p> <p>All staff are asked annually to confirm they have read and understood the Information and Records Management Policy and related procedures and guidance.</p> <p>All members of staff are provided with mandatory data protection training so that they understand their data protection responsibilities when handling personal data.</p> <p>Staff engaged in activities that include records with personal data are also trained so that they understand their responsibilities under data protection</p>

	<p>law.</p> <p>The FAM is supported to attend training and PRSA surgeries in records management.</p> <p>Records are kept of any staff who have completed records management training.</p>
Evidence of Compliance	<p>Evidence submitted in support of Element 12 comprises:</p> <ul style="list-style-type: none"> • Information and Records Management Policy • Information and Records Management Handbook
Future Developments	<p>As part of the annual learning and development planning process, consideration will be given to seeking external training opportunities for the HOCS, FAM and the Administrator.</p>

Element 13: Assessment and review

<p>Introduction</p>	<p>The Public Records (Scotland) Act 2011 provides that an authority must keep its RM Plan under review.</p> <p>An authority's RM Plan must describe the procedures in place to regularly review it in the future.</p> <p>It is important that an authority's RM Plan is regularly reviewed to ensure that it remains fit for purpose. It is therefore vital that a mechanism exists for this to happen automatically as part of an authority's internal records management processes.</p> <p>A statement to support the authority's commitment to keep its RMP under review must appear in the RMP detailing how it will accomplish this task.</p>
<p>Statement of Compliance</p>	<p>The Commissioner's records management systems are reviewed regularly by the HOCS, and the RM Plan, which is key document, is subject to a formal review by the Senior Management Team (SMT)</p> <p>The HOCS is responsible for reviewing the RM Plan and will consult with colleagues and make recommendations to the SMT regarding any updates required. Any changes to be made to the RM Plan need to be approved by the SMT.</p> <p>The Commissioner's Governance Reporting Arrangements require the HOCS to provide an annual assurance report on information and records management to the SMT.</p> <p>The Commissioner also has procedures in place to manage "Key Documents" which ensure key documents, including the RM Plan and the information and records management policies and procedures are reviewed regularly. To assist with reviews, the Review Schedule for Key Documents is considered every two months by the SMT.</p> <p>The IRM Report 2020-21 submitted by the HOCS to the SMT on 12 May 2021 identifies a good level of compliance with our Information and Information and Records Management Policy and the procedures set out in the Information and Records Management Handbook.</p> <p>The Commissioner's Operational Plan 2021-22 incorporates a range of information and records management related activities.</p>
<p>Evidence of Compliance</p>	<p>Evidence submitted in support of Element 13 comprises:</p> <ul style="list-style-type: none"> • Governance Reporting Arrangements • Key Document Handbook • Operational Plan 2021-22 • Committee Report – Information and Records Management and Assurance – submitted to QSMTM on 12 May 2021

Future Developments	<p>A project to consider and recommend a way forward for the management of key documents and reviews is due to be undertaken in 2021-22.</p> <p>COVID –19 pandemic</p> <p>As a result of the impact of the COVID-19 pandemic, the following actions have been taken:</p> <ul style="list-style-type: none">• the office premises have been closed temporarily since 23 March 2020 and remain closed• office security and IT security measures are in place whilst the office premises are temporarily closed• all members of staff are working remotely (with remote access to the office systems) using laptops and mobile phones provided by us and this includes the Commissioner and all members of the SMT• due to the temporary closure of the office premises and limited access to remote working systems, consideration of the Key Documents Review Schedule was deferred in Q1 and commenced again in Q2.• updated guidance has been issued to staff working remotely covering:<ul style="list-style-type: none">○ security of information, including data protection○ records management - staff working remotely must comply with our information and records management procedures including ensuring that our records are trustworthy, complete, accessible, legally admissible in court and robust○ data incident procedures○ how to use Microsoft Teams and guidance on use <p>When the office premises are able to re-open, it is likely that blended/hybrid working will be in place and the guidance issued to staff and any relevant policies and procedures will be updated to take account of the revised arrangements (as necessary).</p>
----------------------------	--

Element 14: Shared Information

<p>Introduction</p>	<p>The Keeper will expect an authority's RM Plan to reflect its procedures for sharing information.</p> <p>Authorities who share, or are planning to share, information must provide evidence that they have considered the implications of information sharing on good records management. An authority's arrangements must, for example, take data protection into account and demonstrate robust arrangements for the safe and secure sharing of personal sensitive data.</p> <p>Information sharing protocols act as high-level statements of principles on sharing and associated issues, and provide general guidance to staff on sharing information or disclosing it to another party. It may therefore be necessary for an authority's RM Plan to include reference to information sharing protocols that govern how the authority will exchange information with others and make provision for appropriate governance procedures.</p> <p>Specifically, the Keeper will expect assurances that an authority's information sharing procedures are clear about the purpose of information sharing which will normally be based on professional obligations. The Keeper will also expect to see a statement regarding the security of transfer of information, or records, between authorities whatever the format.</p> <p>Issues critical to the good governance of shared information should be clearly set out among parties at the earliest practical stage of the information sharing process. This governance should address accuracy, retention and ownership. The data sharing element of an authority's RM Plan should explain review procedures, particularly as a response to new legislation.</p>
<p>Statement of Compliance</p>	<p>The Commissioner complies with data protection requirements in the DPA 2018 and the UK GDPR.</p> <p>We do not have any information sharing arrangements in place.</p> <p>We have a statutory duty to respond to requests for information made under the Freedom of Information (Scotland) Act 2002 and the Environmental Information (Scotland) Regulations 2004.</p> <p>We also have a statutory duty to respond to subject access requests and respond to other requests made under the DPA 2018.</p> <p>We share information, agreed for publication, openly through our publication scheme and Guide to Information. The Commissioner has adopted the Model Publication Scheme (MPS) in its entirety and the Key Document C5 Publication Scheme Handbook sets out:</p> <ul style="list-style-type: none"> (i) the Commissioner's policy on compliance with the publication duties in the Freedom of Information (Scotland) Act 2002 (FOISA) and the Environmental Information (Scotland)

Regulations 2004 (the EIRs)

- (ii) the procedures for publication and maintenance of the Commissioner's Guide to information (GTI).

The Commissioner's GTI:

- (i) allows anyone to see what information is available (and what is not available) in relation to each class
- (ii) states what charges may be applied
- (iii) explains how to find the information easily
- (iv) provides contact details for enquiries and to get help with accessing the information
- (v) explains how to request information that has not been published
- (vi) is regularly and routinely updated

As regards Class 3 (How we take decisions and what we have decided), we publish agenda, Committee Reports (and related papers) and minutes of the SMT meetings where we do not need to withhold information on the basis of the relevant exemptions either in the Freedom of Information (Scotland) Act 2002 or in the Environmental Information (Scotland) Regulations 2004.

The Committee Report (CR) template includes a publication section and a recommendation on publication is being used for all committee reports. This means that decisions about whether to publish information related to matters considered at meetings of the SMT are taken at the point of making the decision and not after the decision.

The Key Document C1 Governance Reporting Arrangements (GRA) requires the HOCS to provide assurance that the Commissioner is publishing and making accessible as much information as possible, in line with the Commissioner's published good practice.

If we were to be required to share any information under a data sharing arrangement, the Commissioner would ensure that the following steps were undertaken:

- the need for, and lawfulness of proposed information sharing, is established before the information is shared.
- the information sharing is documented – generally this would be by means of an information sharing agreement (ISP) or on an instance by instance basis as appropriate.
- a log of information sharing would be retained.
- any information shared would be follow a secure and appropriate process.
- The ISP related to the sharing of personal data is shared, the need for an impact assessment would be considered and this would take account of any transparency requirements for data subjects.

<p>Evidence of Compliance</p>	<ul style="list-style-type: none"> • Data Protection Policy and Handbook • Committee Report – Publication Scheme (SIC) Assurance Report submitted to QSMTM on 4 February 2021 • Publication Scheme – Guide to Information • Publication Scheme Handbook • Governance Reporting Arrangements • Accessibility Statement
<p>Future Developments</p>	<p>Website accessibility</p> <p>The Public Sector Bodies (Websites and Mobile Applications) Accessibility Regulations 2018 ('the Regulations') set out requirements regarding website accessibility and these Regulations build on existing obligations under the Equality Act 2010, which state that all UK service providers must consider "reasonable adjustments" for disabled people. This can include making reasonable adjustments in respect of users of a website who may have impaired vision, motor difficulties, cognitive impairments or learning disabilities and deafness or impaired hearing. The Regulations provide that all public sector bodies must publish an Accessibility Statement that explains how accessible their website is.</p> <p>Whilst some improvements have been made to the Commissioner's website, some parts of it are not fully accessible and this is explained in the Accessibility Statement.</p> <p>There are over 5,000 PDFs on the website, covering a range of topics and types of information and many of which are published under the GTI - historically PDFs are the main tool which has been used to create and share our published documents and information. Making the information in these documents more accessible is likely to have benefits for some disabled people using the website. However, our published documents and information can be made available by other means, wherever possible.</p> <p>As regards the documents and information in our GTI which have been published in a PDF format, it is noted that:</p> <ul style="list-style-type: none"> • the website layout is not responsive, for example, to high zoom, larger spacing or mobile device screens, and, therefore, some content can be lost or can become obscured • documents and information in a PDF format may not be accessible to screen reader users - any document or information published in a PDF created after 23 September 2018 is not exempt from the Regulations • the website can be difficult to navigate using a keyboard as there is no visual focus indicator • some older content including decisions can be difficult to navigate for screen reader users due to incorrect heading structures <p>The Accessibility Statement explains that addressing the issue of</p>

documents and information produced in a PDF format after 2018 would be a disproportionate burden within the meaning of the Regulations. Changing business processes relating to the publication of documents and information in a PDF format on the website would involve a significant amount of work and process change requirements.

Any changes that are made would also need to be considered in the light of our records management processes. Work on establishing how our processes can change is taking place and, in due course, we will make another assessment but this is not likely to be before the end of June 2021. We will continue to ensure published documents and make information available by other means wherever possible.

Website

There is a project within the Operational Plan 2021-22 to procure a new website (with the intention that this will be designed, built and put in place in 2021-22 and 2022-23. Publication arrangements and accessibility requirements will be considered and taken account of in the specification and design of the new website.

COVID-19 pandemic

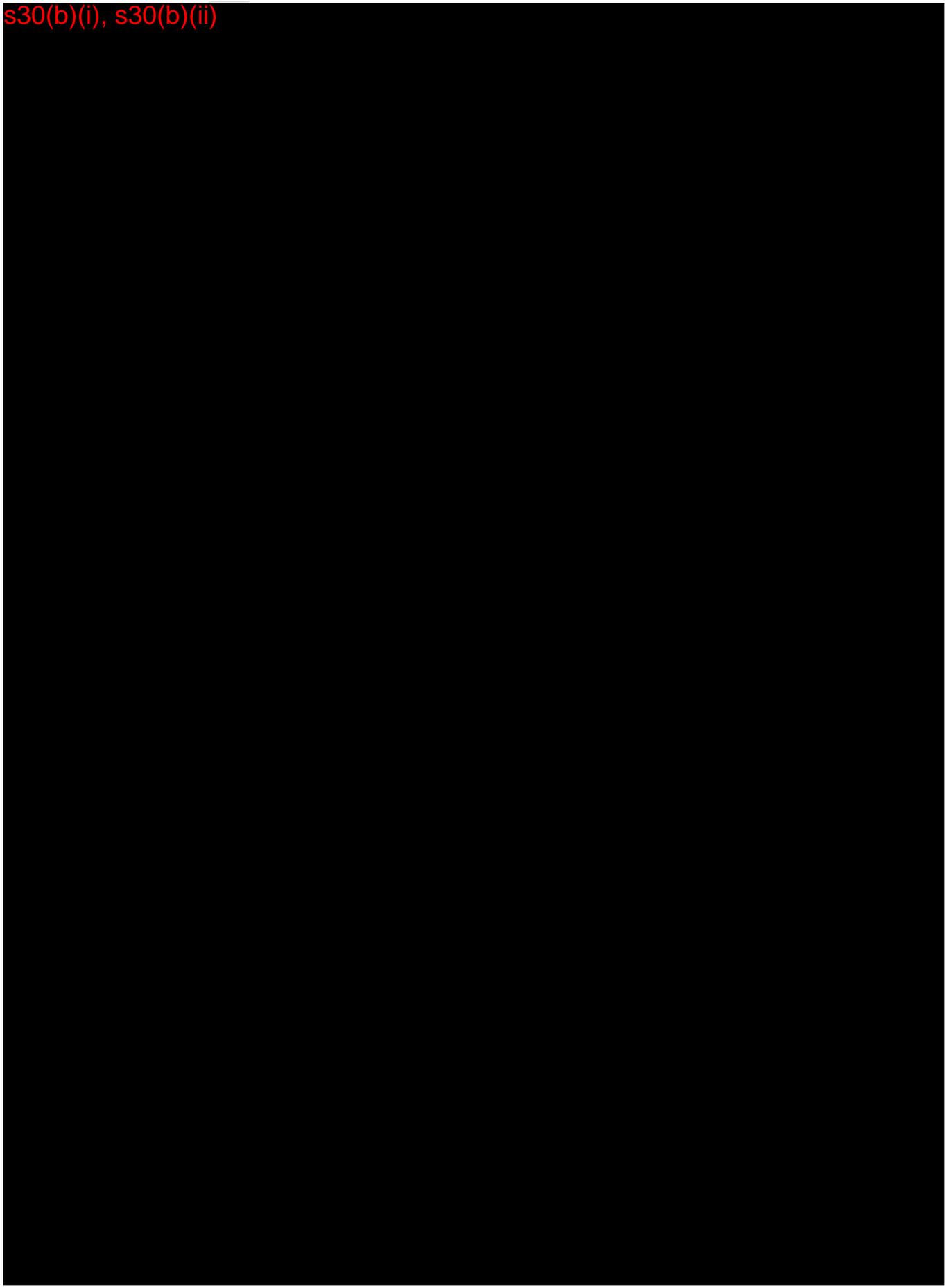
Our priority as an organisation has been to continue to provide key services and guidance within available resource while safeguarding the health, safety and wellbeing of our members of staff.

Since closing our office premises on 23 March 2020 and putting in place our business continuity arrangements, we have worked to maintain operational output and this has included publishing as much information as possible in line with the Commissioner's policy, GTI and governance reporting arrangements.

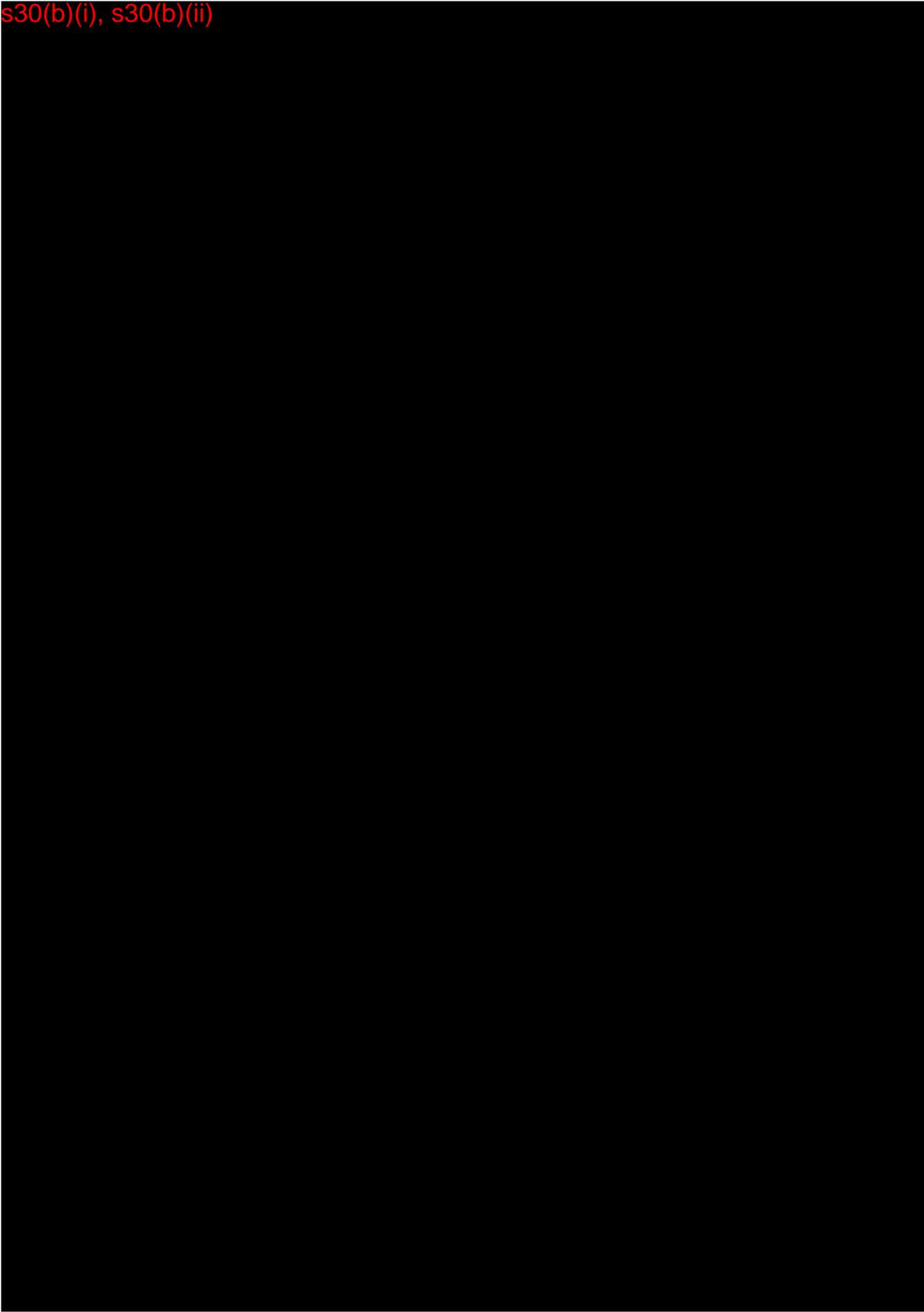
Element 15: Public Records created or held by third parties

<p>Introduction</p>	<p>Adequate arrangements must be in place for the management of records created and held by third parties who carry out any functions of the authority.</p> <p>Section 3 of the Act describes the meaning of ‘public records’ for the purposes of the Act. It says that public records in relation to a named authority means records created by or on behalf of the authority in carrying out its functions. This is extended to records created by or on behalf of a contractor carrying out the authority’s functions and includes records that have come into the possession of the authority or contractor in carrying out the authority’s functions. Records created or held by a third party contractor that are not done so in relation to that contractor carrying out the function of the public authority are not public records under the Act.</p> <p>An authority’s plan must include reference as to what public records are being created and held by a third party carrying out a function of the authority and how these are being managed to the satisfaction of the authority. This does not mean the authority must impose its own arrangements on the third party.</p> <p>Authorities should take a risk-based approach to the arrangements it puts in place with third parties to ensure that these are relevant and proportionate to the public records that fall within the scope of each contract type. Records management requirements, and evidence of assurance that prospective contractors will be able to meet these, should be included in the procurement exercise.</p> <p>An authority will wish to ensure the scope of its proposed arrangements include sub-contractors. It will further wish to ensure that arrangements are in place to allow it to meet statutory obligations under other information legislation, for example, to FOI(S)A and data protection legislation (see Element 9). There may be other regulatory obligations that an authority will wish to consider in relation to the function being carried out by the third party.</p>
<p>Statement of Compliance</p>	<p>N/A – the Commissioner does not delegate any functions to be carried out by third parties</p>
<p>Evidence of Compliance</p>	
<p>Future Developments</p>	

s30(b)(i), s30(b)(ii)

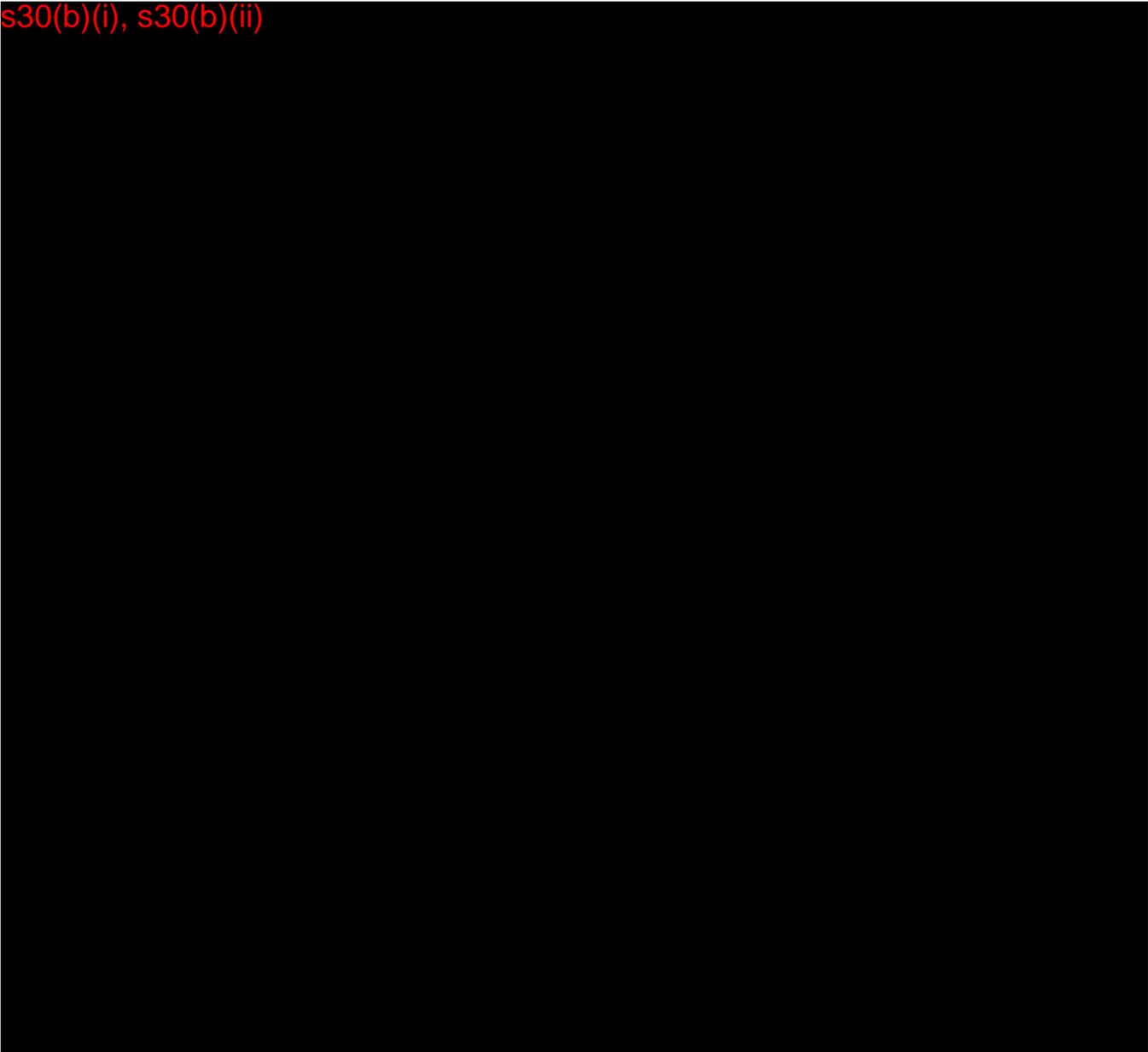


s30(b)(i), s30(b)(ii)



s30(b)(i), s30(b)(ii)

s30(b)(i), s30(b)(ii)



Scottish Information Commissioner

Kinburn Castle
Doubledykes Road
St Andrews, Fife
KY16 9DS

t 01334 464610

f 01334 464611

enquiries@itspublicknowledge.info

www.itspublicknowledge.info

© Scottish Information Commissioner 2021

You may use and re-use this information (not including logos) free of charge in any format or medium, under the terms of the Open Government Licence v3.0. To view this licence, visit <http://www.nationalarchives.gov.uk/doc/open-government-licence/version/3/>