

Public Records (Scotland) Act 2011

Social Care and Social Work Improvement Scotland (The Care Inspectorate)

The Keeper of the Records of Scotland

8 December 2021

Contents

1. Public Records (Scotland) Act 2011	3
2. Executive Summary	4
3. Authority Background	4
4. Assessment Process	5
5. Model Plan Elements: Checklist	6
6. Keeper's Summary	30
7. Keeper's Determination	31
8. Keeper's Endorsement	31

1. Public Records (Scotland) Act 2011

The Public Records (Scotland) Act 2011 (the Act) received Royal assent on 20 April 2011. It is the first new public records legislation in Scotland since 1937 and came fully into force on 1 January 2013. Its primary aim is to promote efficient and accountable record keeping by named Scottish public authorities.

The Act has its origins in *The Historical Abuse Systemic Review: Residential Schools and Children's Homes in Scotland 1950-1995* (The Shaw Report) published in 2007. The Shaw Report recorded how its investigations were hampered by poor record keeping and found that thousands of records had been created, but were then lost due to an inadequate legislative framework and poor records management. Crucially, it demonstrated how former residents of children's homes were denied access to information about their formative years. The Shaw Report demonstrated that management of records in all formats (paper and electronic) is not just a bureaucratic process, but central to good governance and should not be ignored. A follow-up review of public records legislation by the Keeper of the Records of Scotland (the Keeper) found further evidence of poor records management across the public sector. This resulted in the passage of the Act by the Scottish Parliament in March 2011.

The Act requires a named authority to prepare and implement a records management plan (RMP) which must set out proper arrangements for the management of its records. A plan must clearly describe the way the authority cares for the records that it creates, in any format, whilst carrying out its business activities. The RMP must be agreed with the Keeper and regularly reviewed.

2. Executive Summary

This report sets out the findings of the Keeper's assessment of the RMP of The Care Inspectorate by the Public Records (Scotland) Act 2011 Assessment Team following its submission to the Keeper on 24 July 2020.

The assessment considered whether the RMP of The Care Inspectorate was developed with proper regard to the 15 elements of the Keeper's statutory Model Records Management Plan (the Model Plan) under section 8(3) of the Act, and whether in this respect it complies with it and the specific requirements of the Act.

The outcome of the assessment and the Keeper's decision on whether the RMP of The Care Inspectorate complies with the Act can be found under section 7 of this report with relevant recommendations.

3. Authority Background

The Scottish Government set up The Care Inspectorate to provide assurance and protection for people who use care, social work and child protection services in Scotland. They operate out of offices across Scotland, from the Borders to the Islands. They are accountable to Scottish Ministers.

The Care Inspectorate is scheduled by the Public Records (Scotland) Act 2011 as 'Social Care and Social Work Improvement Scotland' which is the Inspectorate's formal name. For the purposes of this report, they will be referred to as The Care Inspectorate.

[Welcome to the Care Inspectorate](#)

4. Keeper's Assessment Process

The RMP was assessed by the Public Records (Scotland) Act Assessment Team on behalf of the Keeper. Assessors used the checklist elements listed in section 5, to establish whether the Care Inspectorate RMP was developed with proper regard to the elements of the Model Plan and is compliant with the Act. The assessment also considered whether there was sufficient supporting evidence of such compliance.

Key:

G	The Keeper agrees this element of an authority's plan.		A	The Keeper agrees this element of an authority's plan as an 'improvement model'. This means that he is convinced of the authority's commitment to closing a gap in provision. He will request that he is updated as work on this element progresses.		R	There is a serious gap in provision for this element with no clear explanation of how this will be addressed. The Keeper may choose to return the RMP on this basis.
----------	--	--	----------	--	--	----------	--

5. Model Plan Elements: Checklist

Element	Present	Evidence	Notes
1. Senior Officer			<p>The Public Records (Scotland) Act 2011 (the Act) requires that an individual senior staff member is identified as holding corporate responsibility for records management in a public authority.</p> <p>Edith Macintosh, Executive Director of Strategy and Improvement, has been identified as the individual with overall strategic responsibility for records management. This is confirmed by a Covering Letter from Ms Macintosh sent with the submitted RMP (evidence 01a)</p> <p>The accompanying letter from Ms Macintosh and the additional e-mail evidence from members of the senior management team, including the CEO, authorising the authority's plan and acknowledging Ms Macintosh's role, is robust.</p> <p>Ms Macintosh, as well as being the Executive Director of Strategy and Improvement, holds the role of Deputy Chief Executive. The authority therefore created the role of Deputy SIRO to take some of the day to day SIRO responsibilities. The job profile for this post (evidence E001b) makes it clear that the Head of Intelligence has shared responsibility for information governance.</p> <p>It is clear from the above that the Executive Director of Strategy and Improvement is alert to and involved in the development of the authority's records management arrangements.</p> <p>The Keeper agrees that the Interim Executive Director of Strategy and Improvement is a suitable individual to adopt this role and therefore agrees this element of the Care Inspectorate's plan.</p>
2. Records Manager			<p>The Act requires that each authority identifies an individual staff member as holding operational responsibility for records management and has appropriate corporate responsibility, access to resources and skills.</p>

			<p>Rachel Mitchell, Information Governance Lead, has been identified as the individual who has operational responsibility for implementing the Care Inspectorate records management plan.</p> <p>This has been confirmed by a <i>Covering Letter</i> from Edith Macintosh, Executive Director of Strategy and Improvement (evidence 03b) April 2020. The letter also confirms Ms Mitchell as the Care Inspectorate’s Data Protection Officer. Ms Mitchell and the IG Lead role are mentioned as being responsible under several other policies and procedural documents supplied in evidence. Ms Mitchell is the author of the <i>Information Governance (IG) Improvement Plan</i> (evidence 03a and 03b).</p> <p>Additional supporting documents, IGL Person Spec, Job profile, PLP and training log, confirm the named person’s roles and responsibilities and the authority’s ambitions for this post. Compliance with the Public Records (Scotland) Act 2011 is identified under this evidence as a specific responsibility. Further, there is evidence of Ms Mitchell’s ‘learning and Development’ goals to remain up to date and in contact with the information governance profession. (evidence E002g)</p> <p>The authority has properly positioned the post of IG Lead within its corporate structure and Ms Mitchell’s appointment ensures it has a professionally experienced officer in post. The Keeper agrees that the named Information Governance Lead is an appropriate individual to undertake this role.</p>
3. Policy			<p>The Act requires an authority to have an appropriate policy statement on records management.</p> <p>The Care Inspectorate has a current <i>Information Governance Policy</i> (IG-001) (version 1.0 dated July 2020) prepared by the Information Governance Team. (evidence 03f).</p> <p>The <i>Information Governance Policy</i> was authorised by the Care Inspectorate Executive Team and is endorsed and owned by the authority’s SIRO, (evidence 03g).</p>

			<p>The <i>Information Governance Policy</i> has been supplied to the Keeper. It is a robust policy which references the Act and other information legislation. It clearly states the importance of good records management to regulatory compliance, business efficiency and the Care Inspectorate’s ambitions as a transparent and trustworthy public body. This is a strong statement which adequately meets the Keeper expectations, fulfils the authority’s obligation under the Act is commended under this Report.</p> <p>The Keeper understands the information governance pages of the authority’s website will be updated in due course and the overarching Information Governance Policy (IG-001), which includes the Data Protection Policy (IG-002) and Records Management Policy (IG-003), will be published at that point. He commends the authority’s ambitions here and looks forward to being informed of this development in due course.</p> <p>The authority has indicated it will publish the agreed plan with the supporting evidence and the Keeper’s assessment internally for the purposes of staff training and communication. This will include ownership of actions to be undertaken to progress the plan and ensure ongoing improvement. This is excellent practice and is welcomed by the Keeper.</p> <p>The Keeper agrees that the Records Management Policy, as a component of the IG Policy, supports the authority’s information governance. Further, it is clear the Information Governance suite of policies are key to its ambitions for the agreed Maturity Model (evidence 03a and 03b). Stage 1 of the Maturity Model has been achieved. Some of the authority’s plans for progress under the Maturity Model were impacted by the Global Pandemic, but this has been assessed and reported and new targets set under a SIRO Report: Risk Reporting Financial Year 2020-2021 (evidence E003i). The Keeper will look forward to learning about progress under the remaining two stages of the Maturity Model.</p> <p>The authority’s holistic approach to improving its information arrangements is an ambitious and comprehensive commitment. It is applauded by the Keeper and he looks forward to learning more about the development and implementation of all the component parts.</p>
--	--	--	--

			<p>The authority has published its suite of information governance policies to its intranet where staff have direct access and includes a ‘published policies’ document as evidence of this (evidence 03d). The additional ‘intranet overview’ document (evidence 03e), combined with the ambition set out under this element to enhance this overall provision to staff, acts as a further indicator of the authority’s commitment to inform staff and make readily accessible all relevant policies.</p> <p>The Keeper agrees that the Care Inspectorate has a robust and operational Information Governance Policy.</p>
<p>4. Business Classification</p>			<p>The Keeper expects that the public records of an authority are known and are identified within a structure.</p> <p>The Care Inspectorate has a Business Classification Scheme (BCS), founded on function. This approach is commended by the Keeper. A functional BCS allows for the incorporation of necessary corporate change without disrupting the classification mechanism.</p> <p>The BCS has been supplied to the Keeper in evidence (evidence 04a). This sets out the authority’s functions, business areas delivering these functions and the classes of records created under each business area. The BCS is supported by BCS Guidance (evidence 04b) which focusses on the authority’s ‘Inspection’ business area as way of demonstrating how staff must interact with the BCS.</p> <p>The authority also has an Information Asset Register (IAR). A redacted version of the IAR is supplied to the Keeper (evidence 04c). The IAR sets out all categories of information and includes columns for retention and key or vital information. This is commendable. Staff are supported when engaging with the IAR by Care Inspectorate guidance (evidence 04d) These structures hold and/or record the authority’s current information assets, regardless of format (physical or digital), but they have not been adequately administered or updated since 2017. Encouragingly, they are currently under close review as the authority transitions to an M365 platform. This transition will enable the authority to fully and comprehensively account for digital records being migrated to the new platform and hard copy records. The</p>

			<p>Keeper will look forward to being updated on progress against this initiative under a future update.</p> <p>The authority has hard copy records stored with an off-site provider. The authority's 'Hard Copy Archive and Records Deposit' form is supplied in support of the current arrangement with its off-site commercial storage provider (evidence 04g). 'Archive' in this context means off-site records storage.</p> <p>The IAR will, in due course, accommodate the authority's Record of Processing Activity (ROPA) to help it better manage its obligations under Data Protection law. (see element 9). The authority's ambitions for this planned incorporation is supported by the Personal Data Audit spreadsheet currently in operation. (evidence 04e).</p> <p>The revision and updating of the authority's BCS/IAR is being undertaken by the IG Team directed by the IG Lead and with critical input from business leads. This work feeds directly into the authority's 'Information Governance Improvement Plan (Maturity Model): Stage 2 Safer and More Secure' (evidence 04i) which seeks to focus on data management and reporting and is a key step towards the authority's goal of achieving an operation Minimum Viable Product output. The Improvement Plan was developed by the IG Lead. It is authorised and owned by the Executive Director of Strategy and Improvement and care Inspectorate SIRO.</p> <p>The authority's plans for progress under the Maturity Model were impacted by the Global Pandemic with some work placed on hold. The authority remained alert to this and recently revised its programme targets. The report on this assessment, which reset timescales against targets, SIRO Report: Risk Reporting Financial Year 2020-2021, was submitted in evidence of planned progress (evidence E003i). Despite obvious restraints, the authority has progressed vital work on information governance. The introduction of One Trust, to host and manage the authority's IAR and ROPA, which has been designed to reflect the authority's BCS and record retention, means progress is being achieved towards the authority's Maturity Model goal. Process activity fields from One Trust are supplied in evidence (evidence E004j).</p>
--	--	--	--

			<p>The authority also has hard copy records which are maintained by commercial off-site storage provider, Iron Mountain. The contract for this service was developed to comply with <i>Crown Commercial Service Framework RM7381: Multifunctional Devices, Managed Print and Content Services and Records Information Management under Lot 4: Records Information Management Services</i>.</p> <p>The Keeper has been provided with details of the third party and of the systems set up with this supplier to ensure he can have confidence Care Inspectorate public records in its keeping are being robustly managed. Evidence includes the procurement information provided by the supplier and assimilated into the contract for the provision of secure off-sight storage, redacted as appropriate (evidence E004k), which specifies compliance with ISO standards on environmental management, ITC, quality management and H&S matters. Security of information is a core service of the third party. In addition the Keeper has been supplied with a copy of the 'Hard Copy Archive and Records Deposit Form' which governs the transfer of hard copy records to the commercial provider (evidence 04g)</p> <p>The authority's records are largely digital, but the Policy says,</p> <p><i>"The Care Inspectorate has adopted a digital-by-default approach. However, where master records need to be retained in physical format, they should be stored within the agreed formal filing structure that conforms to the Care Inspectorate's BCS and related information architecture standards as identified in our hard copy file and retrieval policies"</i></p> <p>The RMP says the authority does not have an on-site hard copy storage facility, but it confirms that staff are required to destroy locally held hard copies of digitally held information in line with the agreed Government Security Classification Procedure (evidence 08a). The plan further confirms that the IG Policy and retention schedule guidance is being amended to emphasise this requirement. The Keeper will be pleased to learn about progress with regard to this initiative under a future update.</p>
--	--	--	--

			<p>The Keeper agrees this element of the Care Inspectorate Records Management Plan under 'improvement model' terms. This reflects the fact that the authority is rolling out a new governance system under its Maturity Model. Evidence submitted satisfies the Keeper that this solution is being progressed and is assured of senior management commitment, but it remains to be fully implemented to cover all business areas. The Keeper's agreement is conditional on his being updated as this work progresses.</p>
<p>5. Retention schedule</p>			<p>The Keeper expects an authority to have allocated retention periods to its public records and for those records to be retained and disposed of in accordance with a Retention Schedule.</p> <p>The Care Inspectorate has a Retention Schedule which supports authority-wide disposal decisions against all record classes. This has been supplied in evidence (evidence 05a)</p> <p>The Schedule supports all record types and formats. A sample entry says, "<i>Estate Management: Building and Facilities Management: Access and security management: Estates, Health & Safety Manager: CCTV footage: Footage date (trigger): 28 days: Statutory: Destroy: Statutory: Data protection Legislation.</i>"</p> <p>The authority's Retention and Disposal Procedure (v2) (evidence 05b) (dated July 2019), created by the IG Lead and owned by the SIRO, is a robust document providing clear and consistent guidance. It addresses all aspects of disposal, including the identification of records of enduring value that require to be transferred to NRS for permanent preservation.</p> <p>The authority, as part of its transition to M365, has completed an assessment and review of its digital assets to apply disposal decisions and prevent the migration of unsuitable and duplicate records to its SharePoint solution. Legacy records on shared drives remain to be similarly reviewed, but this is in hand. The Keeper will be pleased to learn about progress against this initiative under a future update.</p> <p>The Keeper agrees that the Care Inspectorate has a robust Retention Schedule</p>

			<p>providing disposal decisions for all record types created across the authority's business areas.</p>
<p>6. Destruction Arrangements</p>			<p>The Act requires that public records are destroyed in a timely, controlled and secure manner.</p> <p>The authority's IG Policy (evidence 03f) states, "No Care Inspectorate record may be destroyed without appropriate authorisation and due regard to both legal obligations and the Care Inspectorate's Retention Schedule. All destructions of Care Inspectorate records must be logged by the disposing business unit where indicated in the Care Inspectorate's Retention Schedule. Care Inspectorate records must be destroyed securely, in compliance with the Care Inspectorate's procedures." The authority's Records Disposal Form, which confirms that records must not be destroyed without the agreement of the IAO, is supplied in support of this procedure (evidence 06a)</p> <p>Hard copy records, recently transferred into the keeping of a new storage provider will be subject to destruction arrangements as part of the third party contract. The Keeper has been provided with details of the third party and of the systems set up with this supplier to ensure he can have confidence Care Inspectorate public records in its keeping are being robustly managed into destruction as appropriate. Evidence includes the procurement information provided by the supplier and assimilated into the contract for the provision of secure off-sight storage, redacted as appropriate (evidence E004k). Work is ongoing to improve metadata relating to hard copy records to be destroyed to permit the comprehensive application of disposal decisions and create a comprehensive destruction log. This remains to be concluded, but it is a key component of the authorised Maturity Model submitted in evidence. The Keeper notes the ongoing nature of work here and will look forward to learning about progress under a future update.</p> <p>Shredding of Care Inspectorate hard copy records is conducted under a shredding contract to ensure the secure destruction of sensitive waste. Such records are stored on site in secured bins prior to collection and destruction. A destruction certificate has been provided in evidence of the process (evidence 06b and 06c).</p>

			<p>Digital records, recently migrated to the new SharePoint/M365 platform are in the process of having disposal labels applied to facilitate destruction, Legacy arrangements, not compatible with the authority’s agreed retention schedule, have been addressed and a new retention label mechanism is being scrutinised for roll out across the authority’s SharePoint solution. The Keeper commends this approach and looks forward to an update on progress in due course.</p> <p>Back up tapes. In line with industry best practice, the Care Inspectorate’s back up tapes have a retention of 1 year, at which point they can be overwritten and/or destroyed. Evidence of digital record (and digital hardware) destruction is supplied to the Keeper (evidence 06d) This is fully operational and the authority is undertaking a review to bring all back up tapes out with this period under the agreed procedure. The Keeper will look forward to learning about progress under the exercise in a future update.</p> <p>Hardware: Hardware disposal is arranged through a third party provider. The Keeper has been provide with evidence of the processes that support this arrangement and a sample destruction demonstrating the arrangement is operational. (evidence 06d)</p> <p>The Keeper agrees that the Care Inspectorate has arrangements in place to irretrievably destroy paper records, digital information and hardware. The plan tells us that a new retention label mechanism, to address legacy arrangements that are incompatible with the authority’s SharePoint solution, are being developed and rolled out. This will support and enhance the operational effectiveness of the SharePoint solution</p> <p>The Keeper agrees that the Care Inspectorate has robust Destruction Arrangements in place to irretrievably destroy records and hardware as appropriate.</p>
7. Archiving and Transfer			<p>The Act requires that all Scottish public authorities identify a suitable repository for the permanent preservation of records of enduring value. A formal arrangement for transfer to that repository must be in place.</p>

			<p>The compliance statement says ‘<i>This invitation to tender [for off-site storage] was futureproofed to include requirements for transfer to the National Records [of Scotland].</i>’ The Keeper is encouraged to know that records currently in commercial storage will be reviewed to identify those with enduring value and suitable for permanent preservation.</p> <p>The Care Inspectorate web site is being actively harvested by NRS and has been since January 2019. This process was enhanced in September 2020 to include the authority’s twitter feed. A link (here) has been provided to the NRS website demonstrating this arrangement.</p> <p>The focus of the Keeper’s assessment under this Element is on whether an authority has identified a suitable archive repository for its records of enduring value, in line with his ‘Supplementary Guidance on Proper Arrangements for Archiving Public Records’ Resources National Records of Scotland (nrscotland.gov.uk). He needs to be satisfied the authority has arrangements in place to support transfer of records of enduring value to archive.</p> <p>The authority meets the requirement here because it has a formal deposit agreement with the National Records of Scotland supporting the transfer of records of enduring value to the Keeper. The Keeper has been provided with access to the MoU in evidence. The Keeper commends the authority for making this MoU publicly available on its website and thereby promoting public sector transparency. Data Sharing/Memorandums of Understanding (careinspectorate.com)</p> <p>The Keeper agrees the Care Inspectorate has arrangements in place to properly archive its records of enduring value.</p>
8. Information Security			<p>The Act requires that public records are held in accordance with information security compliance requirements.</p> <p>The Care Inspectorate IG Policy commits the authority to good information security. It says, “<i>Our processes use ISO/IEC 27001 and National Cyber Security Centres (NCSC) Software</i></p>

			<p><i>as Service security principles for guidance in defining an asset-based, risk-based approach to information security. The risk assessment process is triggered before each new digital service. We ensure that repeated risk assessments produce consistent, valid and comparable results". ICT Service Team retain documented information about its risk assessment process so that it can demonstrate compliance with these requirements."</i></p> <p>The Keeper is grateful for being provide with evidence of the ICT documents referred to above.</p> <p>The Care Inspectorate, as part of its transition work and its ambitions for better overall information governance, is developing new policies and procedures to address specific information security matters. This includes developing a Government Security Classification Policy, Digital/Cyber Incident Management & Recovery policy and an 'Approach to Digital Security and Risk Management' policy. When finalised these policies will be owned by the Head of Finance and Corporate Governance. The authority will be pleased to have sight of these documents when they are authorised and operational.</p> <p>The authority also draws on generic standards to help it achieve its information security goals, such as the National Cyber Security Centre 10 Steps to Cyber Security (evidence 08e). It further requires its ICT Service Team to comply with an agreed risk assessment process demonstrating compliance with internal information governance policy requirements; Information Risk Governance and Reporting Framework (evidence 08g)</p> <p>The authority is also in receipt of a Cyber Essentials certificate. This is a commendable achievement. The assessment has verified the authority is recorded under the National Cyber Security Centre registration as currently certificated as IASME-CEP-002148 (evidence 08f).</p> <p>The authority's Information Risk Governance and Reporting Framework is a an overall robust document that assists with the identification and management of risk with respect to information security, particularly where new digital services are being adopted (evidence 08g). The Information Risk Governance and Reporting Framework also currently underpins</p>
--	--	--	--

			<p>the authority's initiative to deliver a robust Information Asset Owner (IAO) culture with enhanced accountability in the use of quarterly reporting by the IAO in relation to their assets.</p> <p>The authority's transition to a new operating platform designed to strengthen its information governance, which is being managed under an authorised Maturity Model, is evidence of its ambitions to improve its governance, particularly with regard to its security arrangements. Nevertheless, the plan identifies the authority's need to improve under this element. It says information security, "has been identified as an area of risk by the organisation" as a result of an independent review of the authority's arrangements. The review, conducted by Protection Group International, a digital risk and open source intelligence consultancy, produced the report, 'Cyber Maturity Strategic Roadmap', This has been supplied to the Keeper (evidence E008h). Encouragingly, a new IT service manager has been appointed and new measures have been identified to drive forward progress. An agreed Security Improvement Action Plan (evidence E008i) and a new Data Breach Policy (evidence E009d) have been submitted to the Keeper in evidence.</p> <p>It is clear that the authority is concerned that its information is appropriately managed to remain safe and secure. The IG Policy commits the authority to robust information security and there are robust policies and procedures in place, under review and in development.</p> <p>The Keeper can agree this element of the Care Inspectorate's RMP on an improvement model basis. This means that he is satisfied the authority has identified gaps in its current provision and has submitted sufficient evidence to satisfy him that it is committed to closing them. Securing our public records is of paramount importance and the Keeper recognises the authority is working hard to improve and address the identified risks that currently exist. He will expect the authority to provide him with evidence of progress against these risks under the annual Progress Update Review.</p>
9. Data Protection			The Keeper expects a Scottish public authority to manage records involving personal data in compliance with data protection law.

			<p>The Care Inspectorate RMP says it, “has a comprehensive Privacy Notice available on the Internet ... [and] many policies that are available to advise staff of their obligations in relation to Data Protection Law and Regulations.</p> <p>The Privacy Notice (Core Privacy Notice (careinspectorate.com)) is indeed comprehensive and it links to additional information and guidance. This is good. It is clear also that the Published Policies document (evidence 09a) available to staff on the Intranet carries links to additional relevant policies and procedures.</p> <p>The authority is committed to Data by Design. The IG Policy says, “<i>The GDPR and DPA require that appropriate technical and organisational measures are taken to implement the data protection principles and safeguard individual’s rights. This is known as ‘data protection by design and by default’ previously known as Privacy by Design. This means that the Care Inspectorate is required to integrate data protection into all processing activities and business practices, from the design right through the life cycle to decommissioning.</i>”</p> <p>The compliance statement refers to Care Inspectorate generic DPIA’s which officers are required to amend for the purposes of complying with data protection law, particularly when in engaged in procurement which requires officers to employ SG GDPR clauses. The authority has supplied the Keeper with sight of the Care Inspectorate generic DPIAs as evidence under Element 14. (evidence 14a, b and c)</p> <p>The authority has a Personal Data Audit tool which has been supplied and which is clearly comprehensive. The PDA provides the authority with vital analytical information on the personal data held within each file type across the authority’s business areas. This is a commendable business tool and central to the authority’s commitment to meet its data protection obligations. (evidence 09c). It also has an up to date and robust Data Breach Policy (evidence E009d)</p> <p>The Information Governance Lead holds the role of Data Protection Officer for the authority (evidence 02c)</p>
--	--	--	---

			<p>The plan cites the authority’s ambitions to improve under this Element, particularly in relation to work to be commenced and concluded under the ‘safer and more secure’ stage of the agreed maturity model (evidence 03b). The Keeper applauds the work that has already been concluded under this initiative and that which is to be taken forward. He will look forward to learning more under a future update.</p> <p>The Care Inspectorate has an up to date and accessible Data Protection Policy which is published to the authority’s website. https://www.careinspectorate.com/index.php/publications-statistics/37-corporate-annual-reports-accounts/corporate-policies-and-governance</p> <p>The authority is also registered with the Information Commissioner (Ref: Z2582022). This is a robust way of demonstrating the authority is clearly alert to its obligations under Data Protection law. The Care Inspectorate includes its registration details under its publicly available and recently updated Privacy Notice. https://www.careinspectorate.com/index.php/core-privacy-notice</p> <p>The plan states that “all new staff are required to complete an induction programme which is a blended approach of ‘face to face’ or Teams training and online modules.” There is also an Information Governance induction course which incorporates Data Protection and Records Management. (evidence E012h) There are proposals under development to record this training and upload it to the authority’s Learning Management System (LMS) to be advertise to staff as a continuous training opportunity. This is commendable and the Keeper would welcome an update on progress against this initiative.</p> <p>The authority’s ‘Safer and More Secure’ transformation programme, part of the Maturity Model initiative, includes training for all Information Asset Owners on the principles and accountability associated with their role (evidence E012i). There is also a recently developed mandatory Data Protection training module which forms part of the authority’s LMS to be rolled out Q3-4 Financial Year 21-22. Again, the Keeper commends the authority for its ambitions under this element and will look forward to learning more</p>
--	--	--	--

			<p>about the roll out of this training under a future update.</p> <p>The Keeper agrees that the Care Inspectorate has arrangements in place that allow them to properly comply with data protection legislation.</p>
<p>10. Business Continuity and Vital Records</p>			<p>The Keeper expects that record recovery is an integral part of the authority's business continuity planning.</p> <p>The Care Inspectorate is currently reviewing its business continuity arrangements to update and enhance its current provision.</p> <p>The authority does, however, have robust arrangements currently in place. The Business Continuity Plan Overview (BCP)' (evidence 10a), supplied in support of compliance, is the authority's foundation document underpinning the system of business continuity management. The system relies on each directorate developing and implementing its own Business Continuity Plan, which must have regard the Business Continuity Plan Overview as the authority's authorised policy.</p> <p>The BCP requires officers to use existing authorised risk registers and incident reporting mechanisms to ensure the system works. The authority's Information Risk Governance and Reporting Framework is robust in supporting its BC arrangements and has been submitted to the Keeper in evidence. (evidence 10e).</p> <p>The authority's Business Continuity Officer (BCO) is the Head of Finance and Corporate Governance. This officer is responsible for Business Continuity and advises the authority on compliance ensuring that the BCP and the work of the ICT department are aligned.</p> <p>The authority relies on its Data Breach Policy (evidence E009d) to help it respond to system failures and/or disasters and other emergencies where the authority could be without access to vital systems and information. It also has a 'Recovery Processes' (V3: 2020) workflow charting the processes to be followed in the event of a breach or access failure and to aid recovery. (evidence 10d). This is ISO 22301 aligned. The Data Breach</p>

			<p>policy is owned by the SIRO, Ms Edith Macintosh.</p> <p>The RMP states that arrangements are agreed and are currently being implemented to routinely ensure the ongoing confidentiality, integrity, availability, and resilience of records involving personal data. The authority’s Risk Reporting mechanism (evidence E003i) supports this provision.</p> <p>The Care Inspectorate have hard copy records in off-site storage under contract. The contract for this service was developed to comply with <i>Crown Commercial Service Framework RM7381: Multifunctional Devices, Managed Print and Content Services and Records Information Management under Lot 4: Records Information Management Services</i>.</p> <p>The Keeper has been provided with details of the third party (Iron Mountain) and of the systems set up with this supplier to ensure he can have confidence Care Inspectorate public records in its keeping are being robustly managed. Evidence includes the procurement information provided by the supplier and assimilated into the contract for the provision of secure off-sight storage, redacted as appropriate (evidence E004k), which specifies compliance with ISO standards on environmental management, ITC, quality management and H&S matters. Security of information is a core service of the third party. In addition the Keeper has been supplied with a copy of the ‘Hard Copy Archive and Records Deposit Form’ which governs the transfer of hard copy records to the commercial provider (evidence 04g)</p> <p>The authority undoubtedly takes business continuity seriously. It has a system in place to help it remain alert to business continuity matters. It has positioned the post of BCO at a senior level within the authority and it has provisions in place to help it respond to a system failure.</p> <p>The compliance statement confirms that while the digital transformation programme, moving from on-premise servers with tape back-ups, to storage within the Azure Cloud and digital back up services, continues to progress as planned, the authority will maintain both systems until it has decommissioned all local servers completely. In addition, it has procured third</p>
--	--	--	--

			<p>party digital back-ups of SharePoint sites which contain most of our records that are not stored in applications.</p> <p>The Keeper agrees the Care Inspectorate has robust arrangements in place sufficient to comply with his expectations under this Element. He acknowledges that the authority continues to transition to a new records platform which will roll out and embed new processes, and he'll look forward to learning more about this, but he</p>
<p>11. Audit trail</p>			<p>The Keeper expects an authority to have processes in place to track public records in such a way that their location is known and changes recorded.</p> <p>The Care Inspectorate acknowledges the importance of its information and records being trustworthy from creation to disposal. Its IG Policy says, <i>"it must be possible to prove that records are what they purport to be and who created them, by keeping a record of their management through time. Where information is later added to an existing document within a record, the added information must be signed and dated. With electronic records, changes and additions must be identifiable through audit trails."</i></p> <p>Under the agreed IG Improvement Plan the authority is, as part of the 'Safer and More Secure' module, implementing improved accountability and reporting by IAOs. This is planned to conclude in the financial Year 2020-2021. This work will specifically address on-site storage, to include a registration system to better track hard copy files, and arrangements for homeworkers, with regard to digital and hard copy information. This is commendable and the Keeper will be pleased to learn more about this work progresses.</p> <p>The vast majority of the public records of the Care Inspectorate are created and managed on the authority's current Microsoft/SharePoint solution. This provides the authority with a powerful search facility that allows a user to track all records using a variety of search criteria. (evidence: Microsoft M365 Versioning and Audit policies are supplied in support of this compliance statement).</p>

			<p>The efficiency of the search facility relies on consistent naming of documents when saved as records on the system. To this end, the authority has developed and implemented a Naming Convention to support access and audit purposes. The Naming Convention was authored by the IG Lead and is authorised and owned by the SIRO. It has been supplied in evidence (evidence 11a). The Keeper commends the authority for developing and implementing this robust arrangement.</p> <p>He is further satisfied that staff can readily access this policy under the authority’s intranet ‘Policies, Guidance and Forms’ pages. (evidence 09a)</p> <p>Tracking of off-site storage records is provided by the commercial supplier. The compliance statement is supported by screen-shot evidence of Iron Mountain’s IM Connect information management system (evidence 11b). This system is accessible by Care Inspectorate staff trained in the use of the system and, of course, Iron Mountain staff. Further evidence includes a copy of the Care Inspectorate/Iron Mountain Contract redacted as appropriate (evidence E004k). It is clear this arrangement means the authority can identify, locate and retrieve the records held under contract by the commercial storage provider, and have confidence in access log information.</p> <p>The Keeper recognises the authority’s transition to a new operating platform will further improve its arrangement under this Element, but he agrees it has sufficiently robust operational processes and procedures to meet his requirements with regards to audit trail provision and version control.</p>
<p>12. Competency Framework for records management staff</p>			<p>The Keeper expects staff creating, or otherwise processing records, to be appropriately trained and supported.</p> <p><i>The Plan says, “The Information Governance Team are the Records Management Professionals who provide advice and guidance to the Care Inspectorate and set policy and practice for agreement by the SIRO and the Executive Group. They maintain their professionalism through networking, attendance at external events and training.”</i></p>

			<p>The Care Inspectorate has provided several pieces of evidence that confirm the authority’s commitment to training its IG officer. The IG Lead Person Spec (evidence 02b), the IG Lead Job profile (evidence 02c), the IG Lead PDP (evidence 02d) and personal Training Logs (evidence 02e) have all been supplied to the Keeper and confirm training already undertaken and the authority’s ambitions for the IG Lead and the wider team. In support of wider training to IG staff the Keeper has been supplied with the IG Coordinator Training Record (evidence 12d) and the IG Analyst Training Record (evidence 12f). Some of the training opportunities acted upon by the IG Lead and others are referenced under the Information Governance Dashboard reporting mechanism (evidence 02f). In addition the SIRO confirms a commitment to training under the letter of confirmation (evidence 01.a).</p> <p>The Care Inspectorate’s IG Policy also makes it clear that the authority is committed to good RM and places expectations on all staff. It says, <i>“It is a line manager’s responsibility to make sure that their staff have had adequate training in all aspects of IG, take training opportunities when they are available and are given the time to do so.”</i> It further says, <i>“The IG team are responsible for the development, updating, dissemination and operational delivery of the Information Governance, Records Management and Data Protection policies, procedures, guidance, awareness, and training.”</i> This is an excellent statement which is commended by the Keeper</p> <p>The authority has provided evidence in support of training analysis needs which informed training to all staff on the creation and management of information on the new M365 platform (evidence 12g). The compliance statement confirms that all Care Inspectorate staff are provided with routine training communications and informal and formal training sessions in the new M365 platform have been established.</p> <p>All staff training is operational for the new off-site storage mechanism (evidence 04g).</p> <p>The plan states that <i>“all new staff are required to complete an induction programme which is a blended approach of ‘face to face’ or Teams training and online modules.”</i> There is also an Information Governance induction course which incorporates Data Protection and Records Management. (evidence E012h) In addition, there are proposals under</p>
--	--	--	--

			<p>development to record this training and upload it to the authority’s Learning Management System (LMS) to be advertise to staff as a continuous training opportunity. This is commendable and the Keeper would welcome an update on progress against this initiative.</p> <p>The authority’s ‘Safer and More Secure’ transformation programme, part of the Maturity Model initiative, includes training for all Information Asset Owners on the principles and accountability associated with their role (evidence E012i). There is also now a mandatory Data Protection training module developed and added to the authority’s LMS to be rolled out Q3-4 Financial Year 21-22. Again, the Keeper commends the authority for its ambitions under this element and will look forward to learning more about the roll out of this training under a future update.</p> <p>The Keeper is confident the authority takes the issue of general and IG staff training seriously. He agrees the arrangements in place are sufficient to achieve his agreement. He notes that the authority has ambitions and plans in place to further improve its arrangements and he looks forward to learning more about this under a future update.</p>
<p>13. Assessment and Review</p>			<p>Section 1(5)(i)(a) of the Act says that an authority must keep its RMP under review.</p> <p>The Care Inspectorate’s plan acknowledges that it has not pursued this requirement as robustly as it might in the past. It states, however, and it is clear from the evidence provided, that the current root and branch review of its arrangements needed to facilitate the transition to M365 includes a commitment to assessment and review under this plan.</p> <p>The Keeper acknowledges that arrangements described under this plan confirm the authority is now committed to robust assessment and review procedures being in place and those procedures being subject to continuous and monitored improvement under an authorised maturity model. (evidence 03a and 03b).</p>

			<p>The plan states,</p> <p><i>“the RMP will be reviewed at the end of each quarter, as the Model Records Management plan factors are being incorporated into a maturity model which will now be part of the SIRO quarterly reporting and be submitted annually to the Care Inspectorate’s Audit and Risk Committee. Any risks will also form part of the IG risk register which is owned by the SIRO and overseen by the Executive Group and Audit and Risk Committee to make sure all risks are being assessed and treated where applicable. The IG lead is responsible for making sure that any information risks and issues are reported in a timely manner, and where required, outside the reporting cycle to the SIRO and further escalated as required.”</i></p> <p>This is a robust statement. It commits the authority to a routine and regular review mechanism reporting to senior management which will act as evidence under any future updates to the Keeper. The authority’s commitment is commended by the Keeper and helps assure him of the determination to establish a robust assessment and review process.</p> <p>The reporting process is confirmed in a letter by the SIRO and provided to the Keeper in evidence of the authority’s commitment. (evidence 01.a). The plan is further clear that responsibility for carrying out the records management reviews lies with the Information Governance lead (evidence 02b and 02c)</p> <p>The Care Inspectorate continues to develop the mechanism it will use to deliver the review. It is clear under the plan that it is committed to understanding its performance against information and data management external benchmarks and statutory requirements. Their finished mechanism, to be an internal assessment process, will therefore draw on available tools to include, the Keeper statutory guidance, NHS Data Security and Protection toolkit and the ICO’s Data Protection Self-Assessment. It is committed to having a first iteration of this bespoke mechanism in place by September 2021. It will be used in the first instance to demonstrate the authority’s baseline maturity position and areas for improvement which will be part of an action plan. The Keeper commends this action. He will expect to learn</p>
--	--	--	---

			<p>more about how this is working under an informal progress update review one year after agreement of this plan.</p> <p>The plan clearly commits the authority to keeping its RMP under review and the accompanying confirmatory letter provided by the SIRO assures the Keeper that it will be carried out.</p> <p>The Keeper is satisfied he can agree this element on an improvement basis. This reflects his satisfaction that evidence exists to convince him of the authority’s commitment to comply, but that the system to bring this about and additional evidence remains to be fully developed and implemented. He will expect to be provided with evidence of the fully operational system or an update on progress under a PUR one year after agreement of this plan.</p>
14. Shared Information			<p>The Keeper expects a Scottish public authority to ensure that information sharing, both within the Authority and with other bodies or individuals, is necessary, lawful and controlled.</p> <p>The Care Inspectorate’s compliance statement says, <i>“Any information sharing ... must have a Screening DPIA and where appropriate a DPIA completed. Where required, a Data Sharing Agreement is written in conjunction with our Legal Services team and signed by all parties after review by IG. This follows the principles as laid out in the ICO guidance. Where possible our Data Sharing Agreements, or similar documents are shared on our Internet for transparency.”</i> This is a robust statement.</p> <p>The authority’s IG Policy demonstrates the authority’s understanding of the importance of safe information sharing. It says, <i>“The Care Inspectorate regards the lawful and correct treatment of personal information as of vital importance to maintaining trusted and positive working relationships with the various groups of individuals whose personal data the Care Inspectorate holds and to ethical and successful business practice.”</i></p> <p>It is clear the authority relies on DPIAs to protect its information when sharing. The plan says, <i>“A DPIA enables privacy risks to be identified and mitigated at an early stage by</i></p>

			<p><i>analysing how the proposed uses of personal information will work in practice. It is a consultative process and involves engagement with people who will be working on, or affected by, the project. All staff must, prior to any new initiative, process, or project carry out a DPIA screening assessment followed by a DPIA if potential privacy risks are identified. A screening assessment must also be completed if there is a wholesale change to an existing process, or a new procurement” Evidence of the authority’s Screening Form (evidence 14a) and sample Data Protection Impact Assessment template form (evidence 14b) have been made available to the Keeper.</i></p> <p>In addition, the authority has supplied the Keeper with evidence of its DPIA Guidance (evidence 14c), invitation to tender procedures (evidence 14d) and associated terms and Conditions (evidence 14e) which address DP obligations in this context.</p> <p>The authority has provided links to its published privacy notice and recently agreed DSA’s as evidence of its commitment to secure data sharing. This is strong evidence, not just of the authority’s processes, but of a corporate ambition to be transparent and accountable to its stakeholders.</p> <p>The authority has set down provisions for sharing under ad-hoc circumstance, i.e. outside of core functional activities. That might include sharing information assets with Police Scotland. It has therefore created a sharing assessment on the corporate OneTrust system which supplements the DPIA process. This follows ICO best practice. An example, redacted as appropriate, has been provided to the Keeper in evidence. (evidence E014e)</p> <p>The Keeper is satisfied the Care Inspectorate properly considers records governance when undertaking information sharing He therefore considers this Element to be in full compliance.</p>
15. Public records created or held by third			<p>The Keeper expects a public authority to ensure that adequate arrangements are in place for the management of records created and held by third parties who carry out any functions of the authority.</p>

parties			<p>The Care Inspectorate is clear under its plan that it does not “outsource the creation of any records that are defined as “public records.”</p> <p>The Keeper agrees that this element does not apply to this authority.</p>
---------	--	--	--

Version

This assessment is on the **Social Care and Social Work Improvement Scotland (The Care Inspectorate)** Records Management Plan (the RMP) submitted to the Keeper for his agreement on 24 July 2020. This is the version dated 2020-2021. The development of the RMP was led by the Care Inspectorate’s Information Governance Lead (see Element 2).

The authority’s information governance policy recognises information “ ... *is a key asset for the Care Inspectorate and needs to be valued. Access to reliable, relevant, secure, accurate and timely information underpins all the actions we take and decisions we make when carrying out the work of the Care Inspectorate. Ultimately, it enables intelligence-led scrutiny and assurance of regulated care services in Scotland, helping us deliver our vision that everyone experiences safe, high-quality care that meets their needs, rights, and choices.*” (Information Governance Policy page 2). This is an important recognition and the Keeper commends it.

The RMP mentions the Act and is based on the Keeper’s, 15 element, Model Plan <http://www.nrscotland.gov.uk/record-keeping/public-records-scotland-act-2011/resources/model-records-management-plan>.

Key Group

The Care Inspectorate has clear lines of responsibility established to ensure robust records management decision making is in place, that all decisions are owned appropriately and that the process is properly devolved, overseen and regulated within the authority. The key group in this regard is the Information Governance Team, led by the Information Governance Lead (Element 2). The SIRO (Element 1) has responsibility for ensuring there is a unified approach to information security, information risk and information assurance and the controls in place to address the physical, personnel, information and cyber security.

The SIRO is responsible to the Executive Group which has overall responsibility for ensuring that records are created and managed in all business areas of the authority to robustly and safely meet the needs of the Care Inspectorate in line with organisational policy and regulatory compliance. At a more granular level all line managers are charged with ensuring the Information Governance Policy and all associated Records Management and Data Protection policies, procedures and guidance are understood by their staff and incorporated into routine administrative practices. The Policy makes it a line manager's responsibility to ensure that staff have had adequate training in all aspects of IG, take training opportunities when they are available and are given the time to do so. Further, the authority's Information Asset Owners have overall responsibility for ensuring records within their Directorates are managed according to statutory responsibilities and Care Inspectorate policies.

6. Keeper's Summary

Elements 1 to 15 that the Keeper considers should be in a public authority records management plan have been properly considered by The Care Inspectorate. Policies and governance structures are in place to implement the actions required by the plan.

Elements that require development by The Care Inspectorate are as follows:

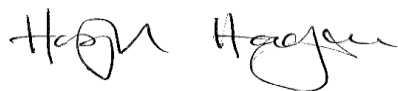
Element 4 Business Classification
Element 8 Information Security
Element 13 Assessment and Review

7. Keeper's Determination

Based on the assessment process detailed above, the Keeper agrees the RMP of **Social Care and Social Work Improvement Scotland (The Care Inspectorate)**

- The Keeper recommends The Care Inspectorate should publish its agreed RMP as an example of good practice within the authority and the sector.

This report follows the Keeper's assessment carried out by,



Hugh Hagan
Head of the Public Records Act team



Liz Course
Public Records Officer

8. Endorsement of Report by the Keeper of the Records of Scotland

The report has been examined and is endorsed under the signature of the Keeper of the Records of Scotland as proof of compliance under section 1 of the Public Records (Scotland) Act 2011, and confirms formal agreement by the Keeper of the RMP as submitted by **Social Care and Social Work Improvement Scotland (The Care Inspectorate)**. In agreeing this RMP, the Keeper expects **Social Care and Social Work Improvement Scotland (The Care Inspectorate)** to fully implement the agreed RMP and meet its obligations under the Act.



.....
Paul Lowe
Keeper of the Records of Scotland