National Records of Scotland

Public Records (Scotland) Act 2011

His Majesty's Inspectorate of Constabulary in Scotland

The Keeper of the Records of Scotland

1st October 2023

Contents

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 His Majesty's Inspectorate of Constabulary in Scotland by the Public Records (Scotland) Act 2011 Assessment Team following its submission to the Keeper on 13th February 2013.

The assessment considered whether the RMP of His Majesty's Inspectorate of Constabulary in Scotland 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 His Majesty's Inspectorate of Constabulary in Scotland complies with the Act can be found under section 7 of this report with relevant recommendations.

3. Authority Background

The Chief Inspector of Constabulary in Scotland (see element 1) is appointed by royal warrant for a term of three years and is personally independent of government and policing bodies. The Chief Inspector fulfils his function through His Majesty's Inspectorate of Constabulary in Scotland (HMICS).

HMICS is an independent scrutiny body, which has been in existence since the nineteenth century. Its role was reaffirmed by the Police and Fire Reform (Scotland) Act 2012, which gave HMICS wide ranging powers to look into the "state, effectiveness and efficiency" of both Police Scotland and the Scottish Police Authority. HMICS can also inspect other UK police services that operate in Scotland. They are also members of the National Preventive Mechanism a group of organisations designated under the Optional Protocol to the Convention against Torture to monitor places of detention and report on the treatment of and conditions for detainees. As part of this body, HMICS inspects police custody centres to monitor the treatment and conditions for detainees.

The last available HMICS Corporate Strategy document is at HMICS | Corporate Strategy 2017-20

For more see HMICS | Home

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 His Majesty’s Inspectorate of Constabulary in Scotland’s 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

His Majesty's Inspectorate of Constabulary in Scotland
(for simplicity this public body will be referred to as 'HMICS' in the assessment below)

Explanation: The records of the HMICS are managed digitally on the Scottish Government's eRDM system and, as this is the case, HMICS must adopt some of the records management provision of the Scottish Government, for example in areas such as information security. This is made clear in the HMICS *Records Management Plan* (*RMP*) for example:

"Whilst His Majesty's Inspectorate of Constabulary in Scotland has its own plan, we continue to follow the Scottish Government's policy and procedures. Therefore this plan will make several references to the Scottish Governments Records Management Plan which has been submitted and approved by The National Records of Scotland" (*RMP* page 2) "His Majesty's Inspectorate of Constabulary in Scotland follow the Scottish Government detailed, Retention and Disposal' Policy." (*RMP* page 13). "His Majesty's Inspectorate of Constabulary in Scotland has adopted the Scottish Governments well-established information security policies and procedures which all staff are required to comply with." (*RMP* page 20).

HMICS previously shared a common *RMP* with the Scottish Government. This was agreed by the Keeper in 2015. Since that time, HMICS have chosen to develop their own *RMP* separately and have submitted that for the Keeper's agreement. The Keeper agrees this is permissible under the Act. However, as noted above, the HMICS *RMP* relies heavily on the records management provision provided by the Scottish Government.

The Keeper last agreed the *RMP* of the Scottish Government in July 2022:
https://www.nrscotland.gov.uk/files//record-keeping/public-records-act/scottish-government-agreement-report.pdf

Element	**Present**	**Evidence**	**Notes**
1. Senior Officer	**G**	**G**	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. His Majesty's Inspectorate of Constabulary in Scotland (HMICS) have identified Craig Naylor, Chief Inspector of Constabulary, as the individual with overall responsibility for records management in the organisation. The identification of the Chief Inspector of Constabulary to this role is supported by the *Records Management Policy* (see element 3), for example in the section 'Responsibilities' and by the *Data Protection Policy* (see element 9), for example in the section 'Management and Responsibilities'. The Chief Inspector of Constabulary acts as the authority's Senior Information Risk Owner (SIRO) and as the Accountable Officer. The Keeper has been provided with the HMICS' *Roles and Responsibilities of the SIRO* document. The primary functions of the role include: a) Lead and foster a culture that values, protects and uses information for the public good b) Own the overall information risk policy and risk assessment process, test its outcome, and ensure it is used Mr Naylor approved the *Records Management Policy*.

			Mr Naylor signed the *Information Security Policy Statement* (see element 8). The HMICS Corporate Services Team, who are "responsible for drawing up guidance for good records management practice", report to the SIRO. The Keeper agrees that His Majesty's Inspectorate of Constabulary in Scotland have identified an appropriate individual to this role as required by the Act.
2. Records Manager	**G**	**G**	The Act requires that each authority identifies an individual staff member as holding operational responsibility for records management and that this staff member has appropriate corporate responsibility, access to resources and skills. HMICS have identified Keri-Anne Balfour, HMICS' Business Support Manager and Records Manager, as the individual with day-to-day responsibility for implementing the *RMP*. The Records Manager reports to the Improvement and Scrutiny Programme Co-ordinator and Senior Information Risk Owner. The Keeper has been provided with Ms Balfour's job description which, among many other administrative roles, includes managing databases and filing systems and updating, maintaining the team's eRDM files and collating information for FOI requests. More specifically she is responsible for maintaining HMICS Records Management Plan as Records Manager. For records management competencies see element 12. The Keeper agrees that His Majesty's Inspectorate of Constabulary in Scotland have identified an appropriate individual to this role as required by the Act.

3. Policy	G	G	The Act requires an authority to have an appropriate policy statement on records management. HMICS have a *Records Management Policy*. The Keeper has been provided with a copy of this *Policy*. This is version 1, dated January 2023. The Policy states in the introduction “HMICS recognises that its records are an important public asset and are a key resource in the effective operation, policy making and accountability of HMICS. Like any asset, records require careful management and this policy sets out HMICS responsibilities and activities in respect of this.” The Keeper welcomes this statement. The *Records Management Policy* has been approved by the Chief Inspector of Constabulary (see element 1). The *Records Management Policy* appropriately informs various aspects of the records management provision in HMICS (see relevant elements below). The Keeper has been provided with a screen-shot showing that HMICS staff can access the Records Management Policy (and other vital information governance instructions). The Keeper agrees that His Majesty’s Inspectorate of Constabulary in Scotland has a formal records management policy statement as required by the Act.
4. Business Classification	G	G	The Keeper of the Records of Scotland (the Keeper) expects that the public records of an authority are known and are identified within a structure.

	🟩	🟩	His Majesty's Inspectorate of Constabulary in Scotland operate a hybrid system: Public records are held digitally on an electronic document and records management system (eRDM), on bespoke line-of-business systems and on shared drives (limited and principally legacy). There are also public records held in hard-copy format in-house (also legacy). Digital eRDM: The vast majority of the public records of HMICS are held on the Scottish Government's eRDM (Objective). The eRDM is provided "to give an office wide information and knowledge sharing resource designed to enable efficiencies in the creation, sharing, retention and retrieval of information. It also enables compliance with related legislative requirements for example Freedom of Information Scotland Act (FoISA) and the Data Protection Act (DPA)." (eRDM Browser Functionality Handbook – see below). The Keeper is familiar with the functionality of this system (it is the one she uses) and agrees that it suitable for the proper management of public authority records. ERDM applies security classification to all files. Security classification can be used to appropriately restrict access (for more on information security see element 8). The Keeper agrees that the arrangement of records in the SG eRDM system, referred to as the 'file plan', acts as a business classification scheme for the authority. The *Scottish Government File Plan* adopted by HMICS has been adapted from the Integrated Sector Vocabulary Scheme Standards | LG Inform Plus (esd.org.uk) and has four levels of classification, the first three levels are subject based and the fourth level describes the activity undertaken. The Keeper is familiar with the structure of the *Scottish Government Business Classification Scheme*. As noted above, it is the one she has chosen to use for the public records of NRS. As evidence of this arrangement, the Keeper has been provided with an extract from eRDM showing an example of an HMICS public record being managed on the system.

	🟩	🟩	This arrangement (that the digital records of HMICS are primarily hosted on the eRDM of the Scottish Government) is confirmed by the HMICS *Records Management Policy* (see element 3); for example at page 5. HMICS have supplied the Keeper with their Business Classification Guidance document which provides a useful explanation of the SG system to their staff. <u>Digital Line of Business</u>: HMICS operate several stand-alone systems for example Egress (information sharing) and SEAS (finance)**.** These line-of-business systems sit outside eRDM, but the Keeper can agree that they are likely to allow the appropriate management of records within a structure as required. HMICS have provided details of the Egress functionality to the Keeper. <u>Digital Shared Drives</u>: a small number of public records remain on a shared drive system. This has been arranged for various reasons, principally because of format incompatibility. HMICS have provided the Keeper with a copy of the *Scottish Government Archival Policy for Shared Drives* statement (2021). The Keeper is familiar with this arrangement and has previously acknowledge it as appropriate. <u>Physical in house</u>: Although the vast majority of HMICS's records are digital, the authority had a paper based records management system until 2014 and still manages legacy files in paper format. Paper records are recorded in the eRDM. The Keeper has been provided with details of the systems in place to ensure that HMICS can be confident that these records can be stored, retrieved and destroyed/archived when appropriate. For example searches can be conducted on file titles (see element 11). <u>E-Mail</u>: HMICS has adopted the Scottish Government's Enterprise Vault to manage

	🟩	🟩	emails. Again this is the same system used by the NRS and so the Keeper is familiar is familiar with its functionality (see element 6). All staff are required to be trained on the use of eRDM before accessing the system and have access to an *eRDM Browser Functionality Handbook*. The Keeper agrees that HMICS staff have access to this *Handbook* through the SG intranet (‘eRDM and Information Management’ page). The Keeper agrees that His Majesty’s Inspectorate of Constabulary in Scotland retains all its public records in a controlled system which is structured in a clear manner and which can be used by staff to manage public records where appropriate.
5. Retention schedule	**A**	**G**	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. The Keeper has been provided with sample file types and retention periods both for HMICS’s administrative records and for their case work. These provide file type, scope, and disposal period for individual record types created by the authority. For example Auditable documents and records relating to the routine management and administration of the HMICS work and activities are closed after 1 year and then destroyed 7 years after closure. The allocation of a record to a file type dictates the retention applied to that record. The involvement of local areas in the allocation of retention is important and happens automatically in eRDM when local Information Management Support Officers (IMSOs) allocate records to file types.

	🟨	🟩	Although the public records of HMICS are now managed digitally, the *RMP* states that retention decisions apply to public records that are managed outside the eRDM, such as legacy paper files (see element 4), This is done by imposing branch/divisional specific retention schedules. The Keeper has been provided with a *Hard Copy File Audit* spreadsheet showing the management of physical records (including retention decsions). **HMICS acknowledge in the RMP that “At the moment they do not use retention and disposal schedules on shared drives, pst files and public folders, but have started a project to look at applying these to our information that does not form part of our corporate record. NRS are part of the board that has been set up for this project.” This statement refers to the Scottish Government’s “Archival Policy for Shared Drives” project. Details have been supplied by HMICS. As noted above, the Keeper is already aware of this work. She accepts that HMICS recognise that retention is not yet satisfactorily applied to a very small section of its public records. However, she is satisfied that there is a clear methodology underway to resolve the issue while sensibly weeding-out records that are of no ongoing business value.** The Keeper acknowledges that the *Subject Access Guidance* document (see element 9) includes retention decisions for SAR requests. **The Keeper can agree this element of His Majesty’s Inspectorate of Constabulary in Scotland’s *RMP* on improvement model terms. This means that the authority has identified a gap in their records management provision (there is a backlog of legacy records that do not have retention/destruction processes applied) and have committed to liaising with the Scottish Government to close that gap. The Keeper’s agreement is conditional on her being kept up-to-date with progress. To this end, the Keeper’s PRSA Team will**

	🟧	🟩	**ensure that a Progress Update Review (PUR) template is provided to HMICS one year after this agreement (and each year subsequently). The PUR process is voluntary, but would provide a suitable opportunity for updating the Keeper on the progress of the back-log project described above:** Progress Update Reviews | National Records of Scotland (nrscotland.gov.uk)
6. Destruction Arrangements	**G**	**G**	The Act requires that public records are destroyed in a timely, controlled and secure manner. HMICS recognise this. They state in the corporate *Records Management Policy* (see element 3): "A systematic approach to the management of HMICS records is essential to protect and preserve records as evidence of our actions. The aim of this policy is to define a framework for managing HMICS records to ensure that we dispose of records that are no longer required in an appropriate manner" (*Policy* page 4) The majority of the public records of HMICS are created and managed on the Scottish Government eRDM system. As this is the case, HMICS "must also ensure that records are maintained and disposed of in accordance with the Scottish Government's records management principles (*Records Management Policy* page 5). Digital (eRDM): Records are automatically deleted according to the retention applied (see element 5) and a 'stub' retained as evidence of destruction. This acts as a destruction log and is to be commended as best practice. The Keeper has previous agreed that the destruction process imposed by eRDM is compliant with expectations under the Act. As evidence of this arrangement, HMICS have provided the Keeper with a screenshot of a destroyed file on eRDM. Paper: Paper records are subject to secure disposal under contract to a third-party

	🟩	🟩	shredding company. A sample destruction certificate has been supplied as evidence that this arrangement is operational. The Keeper acknowledges that the vast majority of HMICS records are managed digitally. Hardware: Destruction of hardware is controlled through the Scottish Government whose hardware destruction procedures have been agreed by the Keeper (July 2022). HMICS have provided the Keeper with a separate statement from the SG to confirm this arrangement. Back-Ups: HMICS, quite properly, keep back-ups of public records for business continuity purposes (see element 10). This is done automatically through the Scottish Government eRDM system. It is important that an authority understands the availability of back-up copies beyond the destruction of the original. HMICS clearly understand this as they have provided the Keeper with the following statement: “The Scottish Government do daily incremental backups and then at the weekend full back ups are taken of the system. The backups are then kept for four weeks and are then destroyed and the information then becomes irretrievable.” She has also been provided with an explanation of the back-up process in eRDM. E-Mail: HMICS has adopted the Scottish Government’s Enterprise Vault to manage emails. Again this is the same system used by the NRS and so the Keeper is familiar with, and approves, its functionality. However, the Keeper is aware that Enterprise Vault is being replaced in the Summer of 2023. She is satisfied that the replacement system will provide similar auto-destruction capabilities albeit with a more generous run-up period. The Keeper agrees that His Majesty’s Inspectorate of Constabulary in Scotland has processes in place to irretrievably destroy their records when appropriate.

7. Archiving and Transfer	**A**	**G**	The Act requires that all Scottish public authorities identify a suitable repository for the permanent preservation of any records considered suitable for archiving. A formal arrangement for transfer to that repository must be in place. HMICS acknowledge this: “A small percentage of HMICS records will be selected for permanent preservation by the National Records of Scotland (NRS) to support historical research” (*Records Management Policy* – see element 3 – page 3) The Keeper agrees that HMICS has therefore identified the National Records of Scotland (NRS) as the repository to which they will transfer the selection of their public records that have been categorised as suitable for permanent preservation. NRS is an accredited archive NRS’ Archive Service Accreditation Success | National Records of Scotland (nrscotland.gov.uk) and fully adheres to the Keeper’s *Supplementary Guidance on Proper Arrangements for Archiving Public Records*: https://www.nrscotland.gov.uk/files//record-keeping/public-records-act/supplementary-guidance-on-proper-arrangements-for-archiving-public-records.pdf **However, at the time of submission a formal transfer agreement had not yet been concluded. The *RMP* states (page 18): “Work still needs to developed on the process around this and a Service Level agreement drawn up.” This has been confirmed by the relevant client manager at NRS.** It is important that an authority has input regarding which of their records might be selected for transfer to archive. The discussion with NRS around the transfer agreement will ensure this involvement in the first instance. Furthermore, the *RMP* states (page 18) that “ERDM will provide us annually with a series of reports which will identify files to be destroyed/kept/reviewed. There will then be a requirement from HMICS to identify those of which need to be preserved/ destroyed and

	🟧	🟩	reviewed". The Keeper agrees this eRDM prompt will be useful to promote the review of the record types identified for permanent preservation. **The Keeper agrees this element of the HMICS Records Management Plan under 'improvement model' terms. This means that the authority has identified a gap in provision (a formal agreement with NRS has yet to be established), but have committed to closing that gap. The Keeper's agreement is conditional on being updated on progress (see PUR under element 5 above).**
8. Information Security	**G**	**G**	The Act requires that public records are held in accordance with information security compliance requirements. "His Majesty's Inspectorate of Constabulary in Scotland has adopted the Scottish Governments well-established information security policies and procedures which all staff are required to comply with. The policies are approved and are reviewed on a regular basis." (*RMP* page 20) The majority of the public records of HMICS are held on the digital systems of the Scottish Government. The SG system is covered by the *Scottish Government Information Security Framework* such as the *Scottish Government Security Classifications* and *Data Handling Standards*. The Keeper has recently reviewed this Framework and agreed is suitable for the protection of public records (July 2022). Legacy paper records are in a Scottish Government building. The Keeper has also agreed that the physical security afforded to records by the Scottish Government is appropriate. HMICS have developed an *Information Security Policy Statement*, signed by the Chief Inspector (see element 1) which has been provided to the Keeper. This is

	🟩	🟩	dated January 2023. The *Policy Statement* supports the use of the SG information security framework and states that “Information is one of HMICS most valuable business assets and needs to be adequately protected against loss or compromise.” The *Information Security Policy Statement* commits HMICS that, using the SG framework, they will ensure that • Information will be protected against unauthorised access. • Confidentiality of information required through regulatory and legislative requirements will be assured. • Integrity of information will be maintained. • Information will be available to authorised personnel as and when required. • Regulatory and legislative requirements will be met. • Business Continuity Plans will be produced, maintained and tested (see element 10). • Information security training will be available to all staff (see element 12). • All breaches of information security, actual or suspected, will be reported to and investigated by the Chief Security Officer. On this last point, the *Information Security Policy Statement* explains the reporting structure in the authority including the involvement of the SIRO (see element 1) This includes actual and potential breaches. The Chief Inspector/Siro has signed that he is content that these objectives are adequately pursued in HMICS. The *Information Security Policy Statement* is specifically format-neutral it covers "physical and IT security and encompasses all forms of information such as data stored on computers, transmitted across networks (including websites and social media), printed out or written on paper, sent by fax, stored on removable media

			such as DVDs and memory sticks..." As well as the *Information Security Policy Statement*, HMICS have developed their own *Clear Desk Policy*. This has been provided to the Keeper. This is the version dated January 2023. The *Clear Desk Policy* reinforces and gives details of the physical security available for the authority's public records (lockable cabinets etc.). HMICS is pro-active in its approach to information risk through the corporate risk register. The Keeper has been provided with a copy of the *HMICS Risk Appetite* statement (December 2020), which she agrees is appropriate for promoting the protection of public records. HMICS undertake annual information security training (see element 12). The Keeper agrees that HMICS staff can access the Scottish Government information security pages through the 'Saltire' intranet. She ha also been provided with screen-shots that demonstrate that Staff can access the *Information Security Policy Statement* and *Clear Desk Policy*, which are specific to HMICS. If the Keeper agrees that His Majesty's Inspectorate of Constabulary in Scotland have procedures in place to appropriately ensure the security of their records as required by the Act.
9. Data Protection	**G**	**G**	The Keeper expects a Scottish public authority to manage records involving personal data in compliance with data protection law. HMICS has adopted the Scottish Governments data protection training and procedures (*RMP* page 22). As the SG is, to some extent, the 'host' of the HMICS public records the Keeper agrees this is appropriate.

			That said, HMICS is registered as a separate data controller with the Information Commissioner's Office (ICO): ZA108009 Information Commissioner's Office - Register of data protection fee payers - Entry details (ico.org.uk) HMICS also have their own *Data Protection Policy*. The Keeper has been provided with a copy of this *Policy*. This is version dated June 2023. The use of personal information and the procedure for making a subject access request is published at HMICS | Data Protection HMICS have appointed a Data Protection Officer (DPO) as required by the Data Protection Act 2018. The HMICS Data Protection Officer is Rhona Ford, Improvement and Scrutiny Programme Co-ordinator. All HMICS staff are required to complete the data protection e-learning module annually (see element 12). The Keeper's own staff follow the same procedure and she therefore agrees that HMICS provide appropriate data protection training. The Keeper has been provided with a screen-shot showing that HMICS staff can access information governance training as appropriate. The Keeper agrees that His Majesty's Inspectorate of Constabulary in Scotland have arrangements in place that allow them to properly comply with data protection legislation.
10. Business Continuity and Vital Records	**G**	**G**	The Keeper expects that record recovery, prioritising vital records, is an integral part of the authority's business continuity planning. HMICS recognise this. They state in the corporate Records Management Policy (see element 3): "A systematic approach to the management of HMICS records is

	🟩	🟩	essential to protect and preserve records as evidence of our actions. The aim of this policy is to define a framework for managing HMICS records to ensure that we Protect vital records” (Policy page 4) The practical operation of business continuity in HMICS must bear in mind the fact that HMICS staff work within a Scottish Government building and the records management provision utilises Scottish Government IT systems. The legacy paper files of HMICS are also housed in SG premises. From the perspective of how the Act applies to business continuity: as the public records of HMICS are managed principally in digital format on the Scottish Government’s eRDM system the authority must depend on the record recovery procedures of the SG. Details of the Scottish Government’s *Back Up Procedures* have been provided (see element 6). HMICS acknowledge that recovery of records in the case of an emergency is a matter for the Scottish Government (*RMP* page 24). The Keeper has already agreed that the Scottish Government has appropriate business continuity procedures in place that will allow for the recovery of records in the case of an emergency. Therefore she is satisfied that appropriate record recovery arrangements are already in place for HMICS’ public records. As the vast majority of HMICS’ public records are held in digital format, and the Scottish Government recovery system should return all records at once, there is no need for HMICS to prioritise the recovery of ‘vital’ records as part of their business continuity arrangements. HMICS have confirmed to the Keeper that none of the legacy paper record still managed on their behalf by the Scottish Government are vital records.

			The Keeper agrees that the His Majesty's Inspectorate of Constabulary in Scotland has procedures in place to ensure the recovery of records in an 'emergency' situation.
11. Audit trail	**G**	**G**	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. With this in mind, HMICS have the following processes in place (For the structure of HMICS' records management systems see element 4 above.) Digital eDRM: The vast majority of the public records of HMICS are managed on the Scottish Government's eRDM platform (Objective). This system has a powerful search facility that allows a user to track all records using a variety of search criteria. The efficiency of the search facility relies on consistent naming of documents as they are saved as records on the system. ERDM automatically inserts version control allowing an authority to identify the correct version of a document. HMICS have provided the Keeper with a separate *Audit Trail* statement confirming this arrangement. As noted above, it is important that HMICS staff name public records consistently. With this in mind HMICS have developed formal naming conventions for their public records and the Keeper has been provided with a copy of their Naming Convention document. This shows record creators how documents should be named to ensure they can be located when necessary. Digital Line-of-Business: HMICS operate line-of-business systems such as Egress. The Keeper can accept these systems have record tracking functionality. Digital Shared Drives: A very small amount of public records are still held on corporate shared drives (usual due to format issues). The Keeper can agree that

			these have been located and identified. Physical in-house: HMICS had a purely paper based records management system until 2014. Legacy paper files have been added to the eDRM and can only be accessed through a controlled system which provides an electronic register of file movement. At any given time the location of a paper record should be immediately identified. Searches can be conducted on file titles (not on the contents). The Keeper agrees that His Majesty's Inspectorate of Constabulary in Scotland has procedures in place that will allow them to locate their records and assure themselves that the located record is the correct version.
12. Competency Framework for records management staff	**G**	**G**	The Keeper expects staff creating, or otherwise processing records, to be appropriately trained and supported. HMICS has adopted the Scottish Governments Competency framework for records management staff which the Keeper has already agreed is an appropriate framework for record managers. The *RMP* (page 28) identifies that the Records Manager will have a degree or post graduate level qualification in information/records management or be working towards such a professional qualification. The individual identified at element 2 has confirmed that she is registered for the University of Glasgow course 'Introduction to Information Management' in 2024 and is undertaking the Data Protection training with Act Now in September 2023. The Keeper agrees that HMICS has allocated appropriate resource to allow their Business Support Manager to undertake the records management aspect of the role. HMICS have confirmed to the Keeper that they will update the text of their compliance statement to recognise the level of training undertaken by the Business Support Manager at the time of the next review (see element 13).

	🟩	🟩	As well as providing the training required by the Records Manager, HMICS are also responsible for ensuring that all staff engaging with public records are sufficiently trained to allow the *RMP* to be implemented. As well as adopting the Scottish Governments Competency framework for records management staff the Keeper notes that they have also implemented training for record creators. For example: All staff at HMICS are required to undertake Protecting Information and Responsible for Information e-learning training alongside specific data protection e-learning training (this is sourced from the Scottish government – see element 9). This annual awareness training reminds employees of the importance of data security and associated risks (*RMP* page 20) All staff are required to complete training on the use of eRDM before they are able to access the system and going forward have access to an *eRDM Browser Functionality Handbook*. The *Handbook* is vital guidance for all aspects of using eRDM from managing e-mails to changing the colour scheme. The Keeper agrees that staff have access to this handbook through the SG intranet (eRDM and Information Management page). Aside from the 'all-staff' mandatory training, HMICS offer e-learning training packages are directed at three different levels of depending on responsibility for records management. The Keeper has been provided with details of training modules in evidence (such as 'Managing Information'). The Keeper is also familiar with the 'Pathways' delivery system for training used by HMICS. The Keeper agrees that the individual identified at element 2 has the appropriate

	🟩	🟩	responsibilities, resources and access to training to implement the records management plan. Furthermore, she agrees that His Majesty's Inspectorate of Constabulary in Scotland consider information governance training for staff as required.
13. Assessment and Review	**A**	**G**	Section 1(5)(i)(a) of the Act says that an authority must keep its RMP under review. HMICS have provided the Keeper with their *Assessment and Review Process* (dated December 2020) which shows that the Corporate Records Manager (see element 2) is responsible for reviewing the implementation of the *RMP* annually and shows how these reviews are reported to senior management. The Corporate Records Manager will be responsible for overseeing the Records Management Plan and making sure that the supporting documentation is kept up to date. It forms part of the Corporate Records Manager's objectives and if documentation is required to be updated it will be updated by the Corporate Records Manager annually and signed off by the Senior Information Risk Owner or they will ask the relevant area in Scottish Government to review and update and this will be signed off by the SIRO. As the public records of the authority are principally managed on the record-keeping systems of the Scottish Government liaising with the SG around systemic review is essential and the Keeper agrees that HMICS have recognised this (*RMP* page 30). **However, there will be a certain amount of local monitoring required of HMICS who are both the record creators and the authority responsible for scrutinising the success of the *RMP*. A process for doing this has yet to be developed. The Keeper would expect HMICS to report on this once the *RMP* has been fully embedded.**

	🟧	🟩	**The *RMP* (page 3) indicates that HMICS will adopt the Keeper’s Progress Update Review (PUR) process (see element 5 for more on the PUR process). This is welcomed and, although voluntary, will provide the authority with an ideal opportunity to update the Keeper around the monitoring of the implementation of the RMP. PUR provides a structured way for authorities to convey the results of a review (either to the Keeper or just internally) it does not suggest <u>how</u> an authority should carry out a review (self-assessment module, staff survey, internal audit etc.). Because of this, the Keeper will require a statement as to how the HMICS Business Support Manager is reviewing the implementation of the *RMP*. For a small organisation, such as HMICS, it may be fairly straightforward to monitor records management processes, however the Keeper cannot fully agree this element of the plan without a statement on this. As the review may be more than a year away, the Keeper will agree this element as an Amber ‘improvement plan’.** HMICS have committed (*RMP* page 9) to ensure that the *Records Management Policy* (see element 3) "will regularly be reviewed in order to ensure that it continues to reflect the organisational position in relation to record keeping.” HMICS commit to reviewing the *Information Security Policy Statement* (see element 8) annually (*Policy Statement* page 3). HMICS commit to reviewing their *Data Protection Policy* annually. The Keeper agrees that HMICS have identified when the RMP will be reviewed, who is responsible for the review and how the results of the review will be reported up to senior management for action. **However, without further information around practicalities of this review she is unable to fully agree this element of the HMICS *RMP*. The Keeper expects to be provided with an update on this aspect of the plan in 2024.**

14. Shared Information	**G**	**G**	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. HMICS have a data sharing agreement with Police Scotland. This is the only data sharing exercise they pursue. The Keeper has been provided with a copy of the HMICS/Police Scotland agreement and agrees that it appropriately considers control of public records as required under this element. Therefore, the Keeper can agree that His Majesty's Inspectorate of Constabulary in Scotland properly considers records governance when undertaking information sharing programmes.
15. Public records created or held by third parties	**G**	**G**	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. The *RMP* makes it clear (page 34) that "His Majesty's Inspectorate of Constabulary in Scotland do contract some of their functions to third parties and use the Scottish Government's call off contract." In July 2022 the Keeper agreed that the framework under which the Scottish Government monitors records created on their behalf by third parties was compliant with her expectations. As HMICS have adopted the processes of the Scottish Government the Keeper is

	🟩	🟩	able to agree that they have properly considered the management of records created by third parties when engaging contractors to undertake activities in pursuance of HMICS functions.

His Majesty’s Inspectorate of Constabulary in Scotland

(for simplicity this public body will be referred to as ‘HMICS’ in the assessment below)

Explanation: The records of the HMICS are managed digitally on the Scottish Government’s eRDM system and, as this is the case, HMICS must adopt some of the records management provision of the Scottish Government, for example in areas such as information security. This is made clear in the HMICS *Records Management Plan* (*RMP*) for example:

“Whilst His Majesty’s Inspectorate of Constabulary in Scotland has its own plan, we continue to follow the Scottish Government’s policy and procedures. Therefore this plan will make several references to the Scottish Governments Records Management Plan which has been submitted and approved by The National Records of Scotland” (*RMP* page 2) "His Majesty’s Inspectorate of Constabulary in Scotland follow the Scottish Government detailed, Retention and Disposal’ Policy." (*RMP* page 13). "His Majesty’s Inspectorate of Constabulary in Scotland has adopted the Scottish Governments well-established information security policies and procedures which all staff are required to comply with." (*RMP* page 20).

HMICS previously shared a common *RMP* with the Scottish Government. This was agreed by the Keeper in 2015. Since that time, HMICS have chosen to develop their own *RMP* separately and have submitted that for the Keeper’s agreement. The Keeper agrees this is permissible under the Act. However, as noted above, the HMICS *RMP* relies heavily on the records management provision provided by the Scottish Government.

The Keeper last agreed the *RMP* of the Scottish Government in July 2022: https://www.nrscotland.gov.uk/files//record-keeping/public-records-act/scottish-government-agreement-report.pdf

General Notes on submission: This assessment is on the *Records Management Plan* (*RMP*) submitted by His Majesty's Inspectorate of Constabulary in Scotland (HMICS) for the agreement of the Keeper of the Records of Scotland (the Keeper) on 13th February 2023.

The *RMP* (page 9) commits HMICS to "Maintain the information in an effective manner whilst ensuring compliance with our legislative requirements." The Keeper agrees that the actions explained in the submitted plan will help the authority pursue that commitment.

HMICS recognise records as a business asset, for example in the *Records Management Policy* (see element 3) Introduction, the *Clear Desk Policy* (see element 8) page 2 or the *Information Security Policy Statement* (see element 8) section 1. The Keeper commends this recognition.

6. Keeper's Summary

Elements ***1 – 15*** that the Keeper considers should be in a public authority records management plan have been properly considered by His Majesty's Inspectorate of Constabulary in Scotland. Policies and governance structures are in place to implement the actions required by the plan.

Elements that require development by His Majesty's Inspectorate of Constabulary in Scotland are as follows

5. Retention schedule
7. Archiving and Transfer
13. Assessment and Review

The Keeper acknowledges that improvement under '5. Retention schedule' is dependent on a Scottish Government project, (which is described in the assessment above) and, as this is the case, is outside the control of HMICS. However, they should ensure that they are fully informed of progress as the project impacts retention decisions being allocated to HMICS' legacy paper records.

7. Keeper's Determination

Based on the assessment process detailed above, the Keeper **agrees** the RMP of **His Majesty's Inspectorate of Constabulary in Scotland**.

- The Keeper recommends that His Majesty's Inspectorate of Constabulary in Scotland 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,

E. Course

…………………………………… ……………………………………

Pete Wadley
Public Records Officer

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 His Majesty's Inspectorate of Constabulary in Scotland In agreeing this RMP, the Keeper expects His Majesty's Inspectorate of Constabulary in Scotland to fully implement the agreed RMP and meet its obligations under the Act.

Laura M. Mitchell.

……………………………………………..

Laura Mitchell
Deputy Keeper of the Records of Scotland