

Public Records (Scotland) Act 2011

NHS Education for Scotland

The Keeper of the Records of Scotland

23rd April 2024

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	38
7. Keeper's Determination	38
8. Keeper's Endorsement	39

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 NHS Education for Scotland by the Public Records (Scotland) Act 2011 Assessment Team following its submission to the Keeper on 13th February 2023.

The assessment considered whether the RMP of NHS Education for 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 NHS Education for Scotland complies with the Act can be found under section 7 of this report with relevant recommendations.

3. Authority Background

NHS Education for Scotland (NES) is an education and training body and a national health board within NHS Scotland. They are responsible for developing and delivering healthcare education and training for the NHS and the health and social care sector. They have a Scotland-wide role in undergraduate, postgraduate and continuing professional development. They also extend their reach to support other public bodies through activities such as the National Trauma Training Programme.

[About NHS Education for Scotland](#)

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 NHS Education for 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

Element	Present	Evidence	Notes
1. Senior Officer	G	G	<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>For the purposes of The Public Records (Scotland) Act 2011 (PRSA) compliance, NHS Education for Scotland (NES) have identified their Chief Executive, Karen Reid as the individual with overall corporate responsibility for records management in the authority.</p> <p>However, the Keeper recognises, and agrees that, for practical purposes, this responsibility has been delegated, by the Chief Executive, to Christopher Wroath, Director of the NES Technology Service and Senior Information Risk Officer (SIRO).</p> <p>This arrangement is confirmed by a separate letter to the Keeper from Mr Wroath, that specifically mentions compliance under the Act. It is also confirmed by the organisation's <i>Records Management Policy</i> and <i>Information Governance Policy</i> (see element 3) under 'responsibilities' (page 5 in both policies) and the <i>Information Security Policy</i> (see element 8) page 6.</p> <p>Mr Wroath reports directly to the Chief Executive.</p> <p>As SIRO, Mr Wroath is the Document Owner of the <i>Records Management Plan</i>.</p>

			<p>The SIRO is the Document Owner of the <i>Records Management Policy</i>.</p> <p>The SIRO is also the Document Owner of the <i>Information Governance Policy</i> (see element 3), the <i>Corporate Records Retention Schedule</i> (see element 5), the <i>Data Cleansing Guidelines</i> (see element 6), the <i>Corporate Information Security Policy</i> and <i>Information Security Acceptable Use Policy</i> (both see element 8) the <i>NES Information Security Manual</i> and the <i>Data Protection, Confidentiality and Privacy Procedures</i> (see element 9).</p> <p>It is clear from the above, that Mr Wroath has considerable direct involvement with the records management provision in NES and is an entirely suitable person to undertake delegated responsibility.</p> <p>The Director of NES Technology Service is a member of the Staff Governance Committee which includes the Chief Executive, NES Executive Directors and Non-Executive Board Members. The Staff Governance Committee ensures senior oversight and accountability of NES policies.</p> <p>The Keeper agrees that NHS Education for Scotland have identified an appropriate individual to this role as required by the Act.</p>
<p>2. Records Manager</p>	<p>G</p>	<p>G</p>	<p>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.</p> <p>For the purposes of PRSA compliance, NES has identified the individual who has operational responsibility for records management as Tracey Gill, Principal Lead Information Governance and Security and the NES Data Protection Officer.</p> <p>"The Information Governance & Security Lead is the senior manager responsible for</p>

			<p>leading the development and implementation of the Information Governance policy and procedures, and for ensuring the separate work streams that underpin Information Governance are implemented in a co-ordinated way to achieve compliance with Information Governance legislation." (<i>Information Governance Policy</i> - see element 3 - page 6)</p> <p>The Information Governance & Security Lead is the author of the <i>Information Governance Policy</i> (see element 3), the <i>Corporate Information Security Policy</i>, the <i>Information Security Acceptable Use Policy</i>, the <i>Incident Notification Management Procedures</i> (see element 8), the <i>Data Protection, Confidentiality and Privacy Procedures</i> and the <i>Data Protection Impact Assessment Guidelines</i> (see element 9). She has also reviewed the <i>Business Continuity Plan</i> (see element 10).</p> <p>The Information Governance & Security Lead is co-author of the <i>NES Information Security Manual</i>.</p> <p>However, the Keeper recognises and agrees that, for practical purposes, the day-to-day implementation of the <i>RMP</i> has been delegated, by the Information Governance & Security Lead to James McCann, Information Governance Programme Officer.</p> <p>This arrangement is confirmed by a separate letter to the Keeper from the NES SIRO (see element 1), that specifically mentions compliance under the Act. The delegation is also confirmed by the organisation's <i>Records Management Policy</i> (see element 3) under 'responsibilities' (<i>Policy</i> page 5).</p> <p>Furthermore, the Keeper has been provided with a copy of the <i>NES Information Governance & Security Business Unit: Roles and Responsibilities</i> document. This makes it clear that, as Programme Officer, Mr McCann is "Responsible for co-ordination of the NES Records Management Plan and annual Progress Update</p>
--	--	--	--

			<p>Review with the Keeper of the Records of Scotland.”</p> <p>Mr McCann reports directly to the Principal Lead Information Governance and Security.</p> <p>The Information Governance Programme Officer is the author of the <i>Records Management Plan</i>.</p> <p>The Information Governance Programme Officer is the author of the <i>Records Management Policy</i> (see element 3).</p> <p>The Information Governance Programme Officer is also the author of the <i>Corporate Records Retention Schedule</i> (see element 5), the <i>Data Cleansing Guidelines</i> (see element 6) and the <i>Document Naming Standards and Version Control Guide</i> (see element 11)</p> <p>For the purpose of PRSA compliance the Keeper recognises Ms Gill, the Information Governance & Security Lead, under this element. The Keeper’s PRSA Team is familiar with Ms Gill and has no doubt of her competence in this role. Furthermore, the Keeper agrees that the Information Governance Programme Officer is an appropriate individual for the practical implementation of the plan.</p> <p>The Keeper agrees that NHS Education for Scotland have identified an appropriate individual to this role as required by the Act.</p>
3. Policy	G	G	<p>The Act requires an authority to have an appropriate policy statement on records management.</p> <p>NHS Education for Scotland have a Records Management Policy which has been supplied to the Keeper. This is version 5.0 approved by Staff Governance</p>

			<p>Committee in August 2022. The author of the <i>Policy</i> is the NES Information Governance Programme Officer who also wrote the <i>Records Management Plan</i>. The <i>Records Management Policy</i> specifically mentions compliance with the Public Records (Scotland) Act 2011 (page 7).</p> <p>The Keeper agrees that the <i>Records Management Plan</i> entirely supports the objectives of the <i>Records Management Policy</i>.</p> <p>The Keeper has been provided with minutes from the meeting of the Staff Governance Committee held on Thursday 11th August 2022 at which the <i>Records Management Policy</i> was approved.</p> <p>NES also operate a separate <i>Information Governance Policy</i>. a copy of this has also been provided. This is version 4.0, created by the Information Governance & Security Lead (see element 2) and approved in November 2020. The Information Governance Policy specifically mentions compliance with the Public Records (Scotland) Act 2011 (page 8). The objective of the <i>Information Governance Policy</i> is to set out the key principles which apply to the management of information stored and used by NES and as such compliments the <i>Records Management Policy</i> (and vice-versa).</p> <p>How the <i>Records Management</i> and <i>Information Governance</i> policies specifically relate to elements of the <i>RMP</i> is noted against the relevant elements below.</p> <p>Staff access to information governance documentation, including formal policies and staff guidance documents, is through the Information & Governance pages of the NES intranet. The Keeper has been supplied with a screen-shot of the Information & Governance homepage and can agree that all relevant documents are available to all staff.</p>
--	--	--	--

			<p>The Keeper agrees that NHS Education for Scotland has a formal records management policy statement as required by the Act.</p>
<p>4. Business Classification</p>	<p>G</p>	<p>G</p>	<p>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.</p> <p>“NHS Education for Scotland (NES) is committed to having an organised and planned approach to the way we manage our organisational records and information” (<i>Data Cleansing Guidelines</i> - see element 6 - section 1).</p> <p><u>Identification of the public records of the authority</u></p> <p><u>Business Classification Scheme</u></p> <p>In the Keeper's original (2013) agreement, this element of the NES Records Management Plan was agreed as an 'improvement model'. The Keeper said: “There is a commitment to develop the classification scheme. The Keeper would be happy to agree this element on an improvement plan basis and would ask to see the updated scheme once implemented.”</p> <p>Since 2013 NHS Scotland boards have collaborated in the development of a central business classification scheme for all boards to adopt. During development NES committed to adopt this scheme. The Keeper acknowledges that she has been kept up-to-date with the development of the national scheme and that a version was made available in late 2021. She agrees that NES has now implemented this scheme. The Keeper acknowledges that a copy of the 2021 scheme has been supplied by NES as part of their <i>RMP</i> evidence package.</p> <p>The NHS Scotland Business Classification Scheme is based on function (rather than business unit). This must remain a decision for the authority, but the Keeper recognises that a functional system, as proposed here, is currently considered best</p>

			<p>practice.</p> <p><u>Information Asset Register</u> NES also has an Information Asset Register that includes all record types held by the organisation, and identifies the Information Asset Owner (see Local Records Management under General Comments below). The register is reviewed annually. A sample of this, very detailed, document has been provided to the Keeper together with a sample of a ‘tracker’ showing how the register is monitored by the information governance team.</p> <p>The Information Asset Register is principally used for mitigating risk and acts as a Record of Processing Activities (ROPA) under GDPR (see element 9).</p> <p><u>Records-Keeping Structure</u></p> <p>NES operates a digital-by-default approach to record creation. The volume of paper-based records is small and continues to reduce as retention periods expire. Since the agreement of NES’s original <i>Records Management Plan</i> in 2013 all health boards in Scotland have committed to the adoption of the Microsoft M365 platform and will, going forward, be utilising the records management functionality in that system. Although the M365 roll-out is not complete nationally, NES was the first NHS Scotland Board to implement M365. M365 is therefore their main repository for corporate records and they no longer rely on traditional shared drives (as they did in 2013). The M365 adoption required NES to map the 2021 <i>Business Classification Scheme</i> (see above) to the M365 structure. The <i>RMP</i> and statements in subsequent engagement with the Keeper’s PRSA Assessment Team, indicates that this has been done.</p> <p>The Keeper acknowledges that NES have correctly identified the importance of appropriate policies, governance and staff training in making the M365</p>
--	--	--	--

			<p>implementation project a success.</p> <p><i>Separately, the Keeper acknowledges that NHS Scotland have provided her with a copy of the SharePoint 'Roadmap' showing how this roll-out will proceed in other Boards.</i></p> <p>A limited number of legacy corporate records were not transferred from Shared Drives to M365. This is because that it has been considered that these records had no business value going forward. There is a current programme of deletion being applied to these records and no new records are created or managed (other than destruction) on shared drives. See under element 6 below for details of the shared drive destruction programme.</p> <p><u>Physical Records</u>: The <i>RMP</i> states: "NES operates a digital-by-default approach to record creation. The volume and significance of paper-based corporate records is small and continues to reduce as retention periods expire. NES has no plans to introduce a manual audit or registry controls for paper records which would be disproportionate to the volume such records held by the organisation". Although NES is principally a digital-first organisation, they are still required to manage legacy records in hard-copy format. It is clear from elsewhere in the <i>RMP</i> that retention and disposition is applied to the small amount of physical records managed by NES (see elements 5, 6 and 7 below) and that physical security is appropriately applied (see element 8). Recently a clear out of on-site paper records was undertaken to reduce to volume of records stored (see element 6).</p> <p>Furthermore NES state: "NES has arrangements in place for legacy paper records to be stored offsite. Requests to store or retrieve records offsite are managed and controlled by Records Management Lead and Programme Officer who are responsible for operational and day-to-day records management.</p>
--	--	--	---

			<p>An inventory of records stored offsite is monitored and maintained by the Information Governance Programme Officer (see element 2). This inventory includes details of the directorates responsible for the of the records throughout their lifecycle, and dates transferred to/retrieved from offsite storage and destruction and disposal. No new records have been moved to offsite storage since August 2019.</p> <p>The Keeper acknowledges that she has been provided with extracts from the NES Offsite Storage Inventory.</p> <p><u>Line-of-Business Systems:</u> NES creates records on line-of-business systems and those records lie outside the main record-keeping systems (TURAS, Finance, HR, IT systems for example). The Keeper acknowledges that she has been provided with information security documentation around the TURAS system. Furthermore, NES have stated: “NES can confirm that records created on line of business systems are captured on the NES corporate records retention schedule. The retention schedule is aligned to the national NHS Scotland business classification scheme & Scottish Government Records Management Health and Social Care Code of Practice (Scotland) 2020.” (<i>Separate Statement</i> provided to the Keeper March 2024).</p> <p>The Keeper also recognises that NES consider the management of other records created outwith the main management systems such as the records of Teams meetings (<i>Information Governance Policy</i> – see element 3 - page 7). These are important considerations and it is commendable that NES formally address these.</p> <p>The Keeper agrees that NES retains all its public records in controlled systems which are structured in a clear manner and which can be used by staff to manage public records where appropriate.</p>
--	--	--	--

<p>5. Retention schedule</p>	<p>G</p>	<p>G</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>NHS Education for Scotland have adopted the <i>Scottish Government Records Management Health and Social Care Code of Practice (Scotland) 2020</i>, which lays out retention decisions for record types created by NHS Boards in Scotland. The Keeper is familiar with the <i>Code of Practice</i> and recognises that her assessment team were informed at all stages of its development. The Keeper agrees that the <i>Code of Practice</i> provides a suitable retention schedule for public records created by NES.</p> <p>The <i>Records Management Policy</i> (see element 3) supports the use of the <i>Code of Practice</i> (for example at pages 4 and 6).</p> <p>The use of the <i>Code of Practice</i> is also supported elsewhere in the evidence package for example in the <i>Data Cleansing Guidelines</i> (see element 6). The <i>Data Cleansing Guidelines</i> also support the implementation of retention to public records (for example at section 2 – which includes a link for staff).</p> <p>As indicated as good practice by the <i>Code of Practice</i>, NES have created their own branded retention schedules based on the retention periods provided and the Keeper has been provided with a copy of the <i>NES Corporate Records Retention Schedule</i>. This is version 2.3 approved by the NES Partnership Forum in January 2022.</p> <p>The <i>NES Corporate Records Retention Schedule</i> is available to all record creators through the authority’s intranet. The Keeper has been provided with screen-shots to confirm this.</p>
------------------------------	-----------------	-----------------	--

			<p>The Keeper notes that NES recognise the risks of public records being created outwith the main record-keeping structure, such as e-mail, Teams or on social media (for example, see <i>Records Management Plan</i> page 12). This is an important recognition and it is important that records created in these systems are properly disposed of either by transfer into the main systems or by secure and timely deletion.</p> <p>In the Keeper's original (2013) agreement, this element of the NES Records Management Plan was agreed as an 'improvement model'. The Keeper said: "The new version [of a retention schedule] will include the identification of vital records. The new schedule may be included in the business classification scheme. Again the Keeper would be happy to agree this element on an improvement plan basis and would ask to see the new schedule, in whichever format it is created, once it has been implemented." The Keeper is now satisfied that, by adopting the <i>Code of Practice</i>, and developing a NES retention schedule available to all staff based on that code, this element of the Records Management Plan is fully compliant.</p> <p>The Keeper agrees that NHS Education for Scotland has a schedule providing retention decisions for the record types created while pursuing its functions.</p>
6. Destruction Arrangements	G	G	<p>The Act requires that public records are destroyed in a timely, controlled and secure manner.</p> <p>In the introduction to the <i>RMP</i>, NES state that “Effective management of information allows fast, accurate and reliable access to records, ensuring the <u>timely destruction of redundant information</u> and the identification and protection of vital and historically important records. Effective records management involves efficient and systematic control of the creation, storage, retrieval, maintenance, use and <u>disposal of records</u>, including processes for capturing and maintaining evidence.”</p>

			<p>One of the principle objectives of records management in NES is "that there are consistent and documented retention and <u>disposal procedures</u> ..." (<i>Records Management Policy</i> – see element 3 - page 6).</p> <p>The <i>Information Governance Policy</i> (see also element 3) commits the authority that "NES will manage the closure, retention and <u>disposal</u> of records, regardless of format" (<i>Information Governance Policy</i> page 9).</p> <p>The secure destruction of records is supported by the <i>NES Information Security Acceptable Use Policy</i> that is issued to all staff, for example at section 8.</p> <p>Similarly, the staff <i>Data Cleansing Guidelines</i> (see below) commits NES as follows: "NHS Education for Scotland (NES) is committed to having an organised and planned approach to the way we manage our organisational records and information. This not only includes efficient storage and retrieval of information, <u>but also the appropriate and effective disposal of redundant information, both electronic and paper</u>" (<i>Data Cleansing Guidelines</i> Introduction)</p> <p>With these policy commitments in mind NES have the following process in place:</p> <p><u>Digital M365</u>: The application of retention and the automation of record destruction in the principle record-keeping system is part of the M365 transition (see under element 4 above) and can therefore be considered operational in NES. They state: "...the implementation of the national BCS through SharePoint labelling functionality and will be linked to retention periods. This will allow for a level of automation of retention and disposal of records, subject to review by staff and the Information Governance team" (<i>RMP</i> page 13). This is an appropriate way forward and the Keeper can agree this as a positive development. The Keeper will be interested in updates as the destruction of public records held in M365 goes live at the end of relevant retention periods.</p>
--	--	--	--

			<p><u>Digital Shared Drives:</u> In the meantime, staff are still encouraged to destroy legacy records that remain held digitally on the now redundant shared drives. This is done through scheduled data cleansing exercises. The Keeper has been supplied with evidence that this exercise was prompted in 2022 and that staff guidance was issued: the NES <i>Data Cleansing Guidelines</i> document (v2.0 2022). The <i>Data Cleansing Guidelines</i> recommend that a data cleansing exercise is undertaken within each business area on a six-monthly basis and no less than annually. The <i>RMP</i> notes that specific records management training (see element 12) may be provided as part of a data cleansing project (this was done for NES Human Resources recently). The <i>Data Cleansing Guidelines</i> specifically mentions compliance with the Act.</p> <p>It is welcome that the ‘weeding’ and manual destruction of public records managed on shared drives was undertaken as part of the implementation of the new centralised system (M365).</p> <p><u>Digital Line-of-Business Systems:</u> NES creates records on line-of-business systems and those records lie outside the main record-keeping systems (TURAS, Finance, HR, IT systems for example). NES have stated: “NES can confirm that records created on line of business systems are captured on the NES corporate records retention schedule. The retention schedule is aligned to the national NHS Scotland business classification scheme & Scottish Government Records Management Health and Social Care Code of Practice (Scotland) 2020.” (<i>Separate Statement</i> provided to the Keeper March 2024). The Keeper accepts that destruction can be applied to these system in accordance with retention decisions.</p> <p>The Keeper can therefore agree that a process for the controlled, secure and irretrievable destruction of all digital records is in place at the time of assessment.</p>
--	--	--	---

			<p><u>Paper in-house</u>: Although NES is developing its digital-first system (see element 4) it must still manage hard copy records to destruction. To this end they have contracted the services of a third-party confidential waste shredding company. All confidential documents are deposited in the confidential waste bins located throughout NES premises for the attention of the third-party contractor. A copy of the service contract has been provided to the Keeper to confirm that this arrangement is in operation. Staff guidance is supplied and has been provided to the Keeper.</p> <p><u>Paper third-party</u>: NES stores some legacy paper records in an offsite storage facility managed by a third-party supplier. NES has controlled arrangements in place for the destruction of these records as the retention periods expire. The Keeper acknowledges that she has been provided with an extract from the NES Offsite Storage Inventory showing the destruction log tab.</p> <p><u>Hardware</u>: Disposal of hardware assets is arranged through the NES Digital Service Desk. The processes for the disposal or cleansing of hardware containing public records is explained in the NES <i>Information Security Manual</i> (see element 8) for example at A.8.3.2 'Disposal of Media'. This is supported in the <i>Information Security Policy</i> (also element 8) for example at page 9.</p> <p><u>Back-Ups (see also element 10)</u>: The Keeper has been provided a copy of the <i>NES Backup Procedures</i> document (v1.0 2021). This explains the backup of public records for business continuity purposes in detail and how long they remain available before the backups are deleted. The NES <i>Information Security Manual</i> also includes procedures for the backup of records.</p> <p>The Keeper agrees that NHS Education for Scotland has processes in place to irretrievably destroy their records when appropriate.</p>
--	--	--	---

<p>7. Archiving and Transfer</p>	<p>G</p>	<p>G</p>	<p>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.</p> <p>In the introduction to the <i>RMP</i>, NES state that “Effective management of information allows fast, accurate and reliable access to records, ensuring the timely destruction of redundant information and the identification and protection of vital and historically important records. Effective records management involves efficient and systematic control of the creation, storage, retrieval, maintenance, use and disposal of records, including processes for capturing and maintaining evidence.”</p> <p>NES state that one of the 'main objectives' of their <i>Records Management Policy</i> (see element 3) is to maintain procedures to include provision for permanent preservation of archival records (<i>Policy</i> page 6).</p> <p>With this in mind, NES have identified the National Records of Scotland (NRS) as an appropriate repository for the preservation of those public records selected as suitable for permanent retention.</p> <p>NRS is an nationally accredited archive NRS' Archive Service Accreditation Success National Records of Scotland (nrscotland.gov.uk)</p> <p>The archiving arrangement is confirmed by an <i>Archive Transfer Agreement</i> between NES and NRS that was formalised in July 2023.</p> <p>NES also have an agreement with the NRS Web Archiving service to routinely harvest NES-owned websites.</p> <p>The Keeper agrees that NHS Education for Scotland has arrangements in place to properly archive records when appropriate.</p>
----------------------------------	-----------------	-----------------	---

<p>8. Information Security</p>	<p>G</p>	<p>G</p>	<p>The Act requires that public records are held in accordance with information security compliance requirements.</p> <p>One of the principle objectives of records management in NES is that “records will be secure from unauthorised or inadvertent alteration or erasure, that access and disclosure will be properly controlled...” (<i>Records Management Policy</i> page 6)</p> <p>The <i>Information Governance Policy</i> requires that NES ensures that “Information is appropriately secured and protected” (<i>Information Governance Policy</i> page 4)</p> <p>NES have an <i>Information Security Policy</i> which has been provided to the Keeper. This is version 5.1 August 2020 reviewed by the NES Information Governance & Security Lead (see element 2). One of the stated objectives of the policy is to “Ensure all information/data, whether manual or digital, is adequately protected against loss, unauthorised access, disclosure or inaccuracy” (<i>Information Security Policy</i> page 4)</p> <p><i>N.B. Subsequent to submission, NES have provided an updated final, approved version of the Information Security policy. Formal approval of the policy was received at the Staff Governance Committee held on 17th August 2023. This is version 6.2</i></p> <p>The Policy is supported by a detailed <i>Information Security Manual</i>. This has also been provided to the Keeper (version 1.0 June 2021) and by a formal <i>Information Security Acceptable Use Policy</i> (v3.0 July 2022).</p> <p>The Keeper has also been provided with sight of the <i>NES Access Control and Back Up</i> (see element 10) guidance documents.</p>
--------------------------------	-----------------	-----------------	---

			<p>The Keeper has been provided with Partnership Forum and Staff Governance Committee minutes approving the information security framework in NES.</p> <p>The Keeper has been provided with a screen-shot showing how NES staff access key information governance policies and guidance including those relating to information security.</p> <p>The Keeper has also been provided with a set of training slides showing the NES 'Information Security What You Need to Know' training module.</p> <p>The Keeper acknowledges that the <i>Information Security</i> and <i>Information Security Acceptable Use</i> policies includes staff guidance on reporting security incidents, actual or potential.</p> <p>The Keeper acknowledges that the <i>Information Security Acceptable Use Policy</i> includes guidance on physical security.</p> <p><u>Line-of-Business systems</u>: NES create and manage records on line-of-business systems, such as TURAS. The Keeper can agree that these are liable to have appropriate information security restrictions, such as access, applied. As a matter of fact, the Keeper acknowledges that she has been provided with information security documentation around the TURAS system.</p> <p>The <i>RMP</i> (page 17) states that "All policies, procedures and systems used to maintain confidentiality, security and integrity of information managed by NES, comply with the NHS Scotland Information Security Framework"</p> <p>The Keeper agrees that NHS Education for Scotland have procedures in place to appropriately ensure the security of their records as required by the Act.</p>
--	--	--	---

<p>9. Data Protection</p>	<p>G</p>	<p>G</p>	<p>The Keeper expects a Scottish public authority to manage records involving personal data in compliance with data protection law.</p> <p>NHS Education for Scotland is registered as a data controller with the Information Commissioner: Information Commissioner's Office - Register of data protection fee payers - Entry details (ico.org.uk)</p> <p>NES publish their data protection principles at Privacy NHS Education for Scotland This includes an clear explanation of how a member of the public can make a subject access request of the organisation.</p> <p>NES have identified their Data Protection Officer. This is the Principal Lead Information Governance and Security Officer (see element 2).</p> <p>The six principles of data protection form part of the organisation's formal <i>Information Governance Policy</i> (see element 3) pages 7/8.</p> <p>NES have provided the Keeper with a sample of their <i>Information Asset Register</i> which acts as their Record of Data Processing Activities (ROPA).</p> <p>NES staff are given instruction on how to report a data protection incident, real or potential, through an incident notification form (see also element 8). A copy of this form has been provided.</p> <p>NES have committed to carrying out data protection impact assessments before they begin any processing of personal data which is likely to result in a high risk to individuals (<i>RMP</i> page 20) With this in mind they have a <i>NES Data Protection Impact Assessment Guidelines</i> document which has been provided to the Keeper. This is version 1.0 dated September 2022. The Keeper has also been provided with</p>
---------------------------	-----------------	-----------------	---

			<p>a screen-shot showing how NES staff access this guidance. Furthermore, “the Data Protection Officer’s advice will be sought when any new information system is being designed to ensure the system’s compliance with NES’s obligations under the Data Protection regulations” (<i>Information Governance Policy</i> page 8).</p> <p>The Keeper has been provided with a copy of the NES ‘Safe Information Handling’ training module which includes staff instruction on protecting personal information.</p> <p>The <i>Records Management Policy</i> – see element 3 – supports appropriate data protection procedures in NES (for example <i>Policy</i> page 4)</p> <p>NES data protection arrangements are supported by their <i>Information Security Policy</i> (see element 8) for example at page 7 and their <i>Data Cleansing Guidelines</i> (see element 6) for example at section 1.</p> <p>The Information Governance & Security team agreed to include Data Privacy and GDPR in the Internal Auditor workplan (see element 13)</p> <p>The Keeper agrees that NHS Education for Scotland have arrangements in place that should allow them to properly comply with data protection legislation.</p>
10. Business Continuity and Vital Records	G	G	<p>The Keeper expects that record recovery, prioritising vital records, is an integral part of the authority’s business continuity planning.</p> <p>The NES <i>Information Security Policy</i> (see element 8) requires NES to “Ensure business continuity plans are produced, maintained and tested periodically” (<i>Information Security Policy</i> page 4)</p> <p>The <i>Information Governance Policy</i> (see element 3) commits NES that “The availability of information systems will be preserved through the operation of clearly</p>

			<p>defined backup procedures and business continuity plans” (<i>Information Governance Policy</i> page 9)</p> <p>The NES <i>Information Security Manual</i> (see element 8) includes procedures for the backup of NES records.</p> <p>With this in mind NES have implemented a <i>Business Continuity Plan</i> which has been provided to the Keeper. This is version 1.2, March 2022. The Keeper agrees that the <i>Business Continuity Plan</i> includes record recovery.</p> <p>The <i>Business Continuity Plan</i> is reviewed annually (see element 13).</p> <p>The NES SIRO (see element 1) is responsible for ensuring the management and maintenance of the <i>Business Continuity Plan</i></p> <p>The overall <i>Business Continuity Plan</i> requires each business area to develop a local “Business Impact Assessments which prioritise the activities, resources and procedures needed to restore services back to a normal level of operation” (<i>RMP</i> page 7).</p> <p>NES has included a copy of two example business impact assessments relating to two different directorates. These are dated 2023 and the Keeper can agree that they both appropriately consider record recovery.</p> <p>The Keeper notes that both the <i>Business Continuity Plan</i> and local <i>Business Impact Assessments</i> are currently under review to take account of changed working practices.</p> <p>A copy of the most recent NES Backup Procedures, which were reviewed in June</p>
--	--	--	--

			<p>2023, have been supplied to the Keeper’s Assessment Team subsequent to submission of the reviewed <i>RMP</i> (see under element 13 for more on the provision of up-to-date versions of documents).</p> <p>The Keeper agrees that NES have an approved and operational business continuity process and that information management and records recovery properly feature in the authority’s plans.</p>
11. Audit trail	G	G	<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>In the introduction to the <i>RMP</i>, NES state that “Effective management of information allows fast, accurate and reliable access to records, ensuring the timely destruction of redundant information and the identification and protection of vital and historically important records. Effective records management involves efficient and systematic control of the creation, storage, retrieval, maintenance, use and disposal of records, including processes for capturing and maintaining evidence.”</p> <p>One of the principle objectives of records management in NES is "that records and the information within them can be efficiently retrieved by those with a legitimate right of access, for as long as the records are held by the organisation..." and that "...audit trails will track all use and changes, and that records will be held in a robust format which remains readable for as long as records are required" (<i>Records Management Policy</i> page 6).</p> <p>The <i>Information Governance Policy</i> (also element 3) confirms that one of the "principles drive activities relating to effective information governance within NES" is that "Information is accessible and preserved for as long as required" (<i>Information Governance Policy</i> page 4)</p>

			<p>NES clearly recognise the importance of having systems in place to locate and identify public records.</p> <p><u>Digital Records Shared/drives/M365</u>: In the Keeper's original (2013) agreement, this element of the NES Records Management Plan was agreed as an 'improvement model'. The Keeper said: "The implementation of Alfresco ECMS will cover the audit trail requirements for the electronic records created by NES. They also intend to apply audit facilities to databases and unstructured information." The Keeper understands that the implementation of the Alfresco ECMS identified in the authority's original, agreed, <i>RMP</i> has now been substituted for M365 as part of a national NHS Scotland roll-out. The Keeper can agree that the M365 platform has a robust search/audit trail facility (e-discovery) that can be utilised in much the same way as the Alfresco system would have been if the original plan had been implemented.</p> <p>The M365 system will automate version control but, in order to fully utilise the powerful e-discovery search functionality, consistent document naming must be imposed on record creators. The Keeper acknowledges that she has been provided with the NES <i>Document Naming Standards and Version Control Guide</i>. This is version 3.0 created by James McCann (see element 2) and approved in April 2022. This is available to NES staff on the intranet and the Keeper has been provided with a screen-shot evidencing this.</p> <p>The <i>Document Naming Standards and Version Control Guid</i> notes that "The principle of naming conventions is to use standard rules that are applied to all documents and electronic folders that contain these documents, in order to enforce consistency in the form of name and in the words used. Implementing good standards in document names will help users to;</p> <ul style="list-style-type: none"> • Quickly access and retrieve electronic documents, • Allow the sorting of documents in a logical sequence (e.g. version number, date),
--	--	--	--

			<ul style="list-style-type: none"> • Help keep track of document versions and avoid unnecessary duplications, • Quickly and easily share information with colleagues across NES.” The Keeper agrees this statement. <p><u>Digital Records Line-of-Business:</u> NES create records on line-of-business systems and that those records lie outside the main record-keeping systems (TURAS, Finance, HR, IT systems for example). For the reasons noted under other elements above, the Keeper can agree that these line-of-business systems are liable to include appropriate record tracking functionality.</p> <p><u>Physical records:</u> Since the COVID-19 pandemic in 2020, NES now operates a hybrid working model with the majority of staff working from home, therefore minimal paper records are now generated on-site. Furthermore, a clear-out of NES offices was undertaken to remove filing cabinet and storage for paper records as the organisation implemented hybrid working. For more on this see element 6 above.</p> <p>NES has arrangements in place for legacy paper records, which are stored offsite, to be destroyed once the agreed retention periods expire. This process is managed and controlled by the Principal Lead/Data Protection Officer, and Information Governance Programme Officer who are responsible for operational and day-to-day records management.</p> <p>An inventory of records stored offsite is monitored and maintained by the Information Governance Programme Officer. This includes details of the directorates responsible for the of the records throughout their lifecycle, and dates transferred to/retrieved from offsite storage and destruction and disposal.</p> <p>A statement from the NES SIRO (see element 1) outlining the organisation’s position on the traceability of paper records is included as part of a supplementary evidence submission. In this letter the SIRO confirms the arrangements noted</p>
--	--	--	--

			<p>above and refers to active paper records being scanned into the SharePoint system (this particular programme of work is not mentioned in the RMP, but is entirely appropriate as part of the digital-first system explained elsewhere).</p> <p>The Keeper agrees NES has procedures in place that will allow them to locate their records and assure themselves that the located record is the correct version.</p>
<p>12. Competency Framework for records management staff</p>	<p>G</p>	<p>G</p>	<p>The Keeper expects staff creating, or otherwise processing records, to be appropriately trained and supported.</p> <p>Tracey Gill, the NES Principal Lead Information Governance and Security, has worked closely with the Keeper's PRSA team for many years and is a highly experienced records manager. The Keeper has no concerns regarding her competence to undertake the lead role in records management in NES.</p> <p>The Information Governance Programme Officer, who has been delegated day-to-day operational responsibility for implementing the <i>RMP</i>, is appropriately trained to Practitioner Level in Scottish Public Sector Records Management. The Keeper thanks Mr McCann for providing his certificate in evidence.</p> <p>The <i>Records Management Policy</i> (see element 3) commits NES to ensure "that all staff are made aware of their record-keeping responsibilities through generic and specific training programmes and guidance" (<i>Records Management Policy</i> page 6)</p> <p>There is also a further commitment in the <i>Records Management Policy</i> that all NES staff will receive basic training to Foundation level in the NHS Scotland Information Governance Competency Framework. The Keeper is familiar with this framework and acknowledges that her PRSA Team have been kept informed of its development (more about the development of this framework is available at Cohort 18 - Information Governance Competency Framework for Health & Social Care -</p>

			<p>Amy Leckie Turas Learn (nhs.scot)</p> <p>The provision of “direction and guidance to NES colleagues” is committed to in a separate letter received by the Keeper from the NES SIRO (see element 1).</p> <p>The <i>Information Governance Policy</i> (see element 3) states that "The following principles drive activities relating to effective information governance within NES...Staff are trained in information governance procedures" (<i>Information Governance Policy</i> page 4, also supported at page 6)</p> <p>With these commitments in mind, a SharePoint Communications site (Information Governance & Security Hub) was launched to all staff in November 2021. This is learning resource which contains all information governance policies, procedures and guidance. The Keeper has been provided with a screen-shot of this site as part of the evidence package accompanying the <i>RMP</i>. Staff are also updated to records management developments directly by e-mail. The Keeper has been provided with an example of this in the form of an <i>Updated NES Records Management Policy All-Staff Communication</i>.</p> <p>NES staff undertake a series of mandatory information governance training modules annually. This includes compulsory data protection refreshers, available through the Information Governance & Security Hub. An example of a training module has been supplied. This is the ‘Safe Information Handling’ module which was launched in 2021 and which all staff are required to complete annually. This sets out the principles for handling sensitive/confidential records or those containing patient data (see element 9).</p> <p>Communications are regularly issued to staff reminding them to complete their mandatory training. The Keeper has been provided a sample reminder e-mail. The</p>
--	--	--	---

			<p>communication of information security developments is a specific requirement of the NES <i>Information Security Policy</i> for example at pages 6 and 7. The Keeper has also been provided with a set of training slides showing the NES ‘Information Security What You Need to Know’ training module.</p> <p>Since 2020, the Information Governance & Security team have also delivered a rolling programme of information security and data protection webinars (information security training is a specific requirement of the NES <i>Information Security Policy</i> for example at ‘Objectives’ page 4). In June 2021 a separate rolling programme of records management training webinars, including a Q&A session, was also implemented. Bespoke information governance training is also available by request.</p> <p>The retention schedule (see element 5) is promoted to staff in information governance communications and the records management training webinars.</p> <p>The Keeper agrees that the individual identified at element 2 has the appropriate responsibilities, resources and skills to implement the records management plan. Furthermore, he agrees that NHS Education for Scotland consider information governance training for staff as required.</p>
<p>13. Assessment and Review</p>	<p>G</p>	<p>G</p>	<p>Section 1(5)(i)(a) of the Act says that an authority must keep its RMP under review.</p> <p>The <i>RMP</i> will be reviewed annually.</p> <p>The NES Information Governance Programme Officer (see element 2) is responsible for ensuring the review is carried out. This is supported by commitments in the <i>Records Management Policy</i> (see element 3), for example at page 7.</p> <p>The Information Governance Programme Officer is supported in this review by the</p>

			<p>organisation’s audit team who have added Information Lifecycle Management (including the Information Asset Register and Retention Schedule) and the <i>Records Management Plan</i> itself to their workplan. The use of a reviewer that sits outside the records management team is commended. NES have supplied the Keeper with a relevant sample of a NES Audit review as evidence (this example is on data privacy).</p> <p><i>The Keeper notes that the NES internal audit cycle has recently been interrupted in response to altered priorities caused by the pandemic. She would appreciate an update on information governance audits when appropriate.</i></p> <p>NES use the Keeper’s voluntary Progress Update Review (PUR) process as a reporting methodology and she acknowledges that her assessment team have been in receipt of completed PURs in recent years. She is pleased to note that NES publish PURs. For example Self-Assessment Mechanisms - Progress Update Review - NHS NES</p> <p>The <i>Records Management Policy</i> commits NES that “the application of records management procedures are regularly monitored against agreed standards and action taken to improve standards as necessary” (<i>Policy</i> pages 6/7).</p> <p>The <i>RMP</i> (page 17) notes that “In November 2020 the Scottish Government undertook a desktop Network and Information Systems (NIS) Regulations audit. A progress audit was undertaken on 1st December 2021 and 16th November 2022”</p> <p>The <i>Records Management Policy</i> is scheduled for review by August 2024.</p> <p>The <i>Document Naming Standards and Version Control Guide</i> (see element 11) is scheduled for review by April 2024.</p>
--	--	--	--

			<p>The <i>Data Cleansing Guidelines</i> (see element 6) will be reviewed every 2 years, next scheduled for review by May 2024.</p> <p>The <i>Business Continuity Plan</i> and business impact assessments (see element 10) are reviewed annually.</p> <p>The most recently approved and published final versions of the <i>Information Governance</i> and <i>Information Security</i> policies have been provided to the Keeper’s Assessment Team subsequent to the submission of the reviewed <i>RMP</i>. Formal approval of these policies was received at the Staff Governance Committee held on 17th August 2023. The Keeper thanks NES for keeping their submission constantly up-to-date in this way and, although these documents are not routinely scrutinised outside the assessment process, it is valuable that the Keeper has the latest versions on file for reference.</p> <p>The <i>Information Security Acceptable Use Policy</i> is currently under review and will be submitted for formal re-approval in line with the NES governance arrangements later this year. As noted above, the Keeper would welcome being provided with a copy of these policies when in order to keep the NES submission up-to-date.</p> <p>The Keeper agrees that NHS Education for Scotland have made a firm commitment to review their <i>RMP</i> as required by the Act and have explained who will carry out this review and by what methodology. Furthermore he agrees that supporting policy and guidance documents have appropriate review periods allocated.</p>
14. Shared Information	G	G	<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>As part of carrying out its function, NHS Education for Scotland shares information with third parties and does so using the NHS Scotland Information Sharing Toolkit. The Keeper is familiar with the 'toolkit' and agrees that it provides a secure and controlled information sharing methodology for NHS boards.</p> <p>Data sharing agreements are recorded in a <i>Data Sharing Register</i>. An extract from that <i>Register</i> has been provided.</p> <p>NES have also provided the Keeper with a sample <i>Information Sharing Agreement Template</i>.</p> <p>The Keeper can agree that NHS Education for Scotland properly considers records governance when undertaking information sharing programmes.</p>
<p>15. Public records created or held by third parties</p>	<p>N/A</p>	<p>N/A</p>	<p>The Public Records (Scotland) Act 2011 (PRSA) makes it clear that records created by third parties when carrying out the functions of a scheduled authority should be considered 'public records' - PRSA Part 1 3 (1)(b).</p> <p>NES state in their <i>RMP</i> (page 33): "NES does not currently have any functions performed by third parties. However, some activities such as payroll and recruitment are managed under the NHSScotland umbrella."</p> <p>The Keeper has determined that payroll and recruitment etc. are services contracted-in to help the organisation pursue its functions, but are not functions in themselves.</p> <p>This element does not apply to NHS Education for Scotland.</p>

NHS Education for Scotland
(Referred to as NES in the assessment below)

General Notes on submission: This assessment is on the reviewed *Records Management Plan (RMP)* submitted by NHS Education for Scotland for the agreement of the Keeper of the Records of Scotland (the Keeper) on 14th February 2023. This is *RMP* version 1.0 approved by Director of the NES Technology Service and Senior Information Risk Owner (SIRO) on 3rd February 2023.

The Keeper has been provided with a separate letter from the NES Director of the NES SIRO, dated February 2023, endorsing the *RMP* and the *Records Management Policy* (see element 3).

This is the second formal records management plan received from NHS Education for Scotland by the Keeper. The first was agreed on the 21st August 2013: <https://www.nrscotland.gov.uk/files/record-keeping/public-records-act/NHSEducationForScotlandAssessmentReport.pdf>

The original *RMP* is available on the NES website as a link from: [Freedom of information | NHS Education for Scotland](#): The Keeper commends the publication of an authority's *RMP* and hopes that NES will similarly publish this new, reviewed, version.

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>. The *Records Management Policy* – see element 3 – also mentions the Act.

The authority refers to records as a business asset (for example *Records Management Policy* - page 4, *Information Governance Policy* page 4 or *Information Security Policy* page 5). This is an important recognition and the Keeper commends it.

NES state that "Records management, through the proper control of the content, storage and volume of records, reduces vulnerability to legal challenge or financial loss and promotes best value in terms of staff time and physical and electronic space through coordination of information and storage systems" *Records Management Policy* - page 4. The Keeper entirely agrees.

The *RMP* (page 3) notes that the “Systematic management of records allows organisations to:

- know what records they have, and locate them easily
- increase efficiency and effectiveness
- make savings in administration costs, both in staff time and storage
- support decision making
- be accountable
- achieve business objectives and targets
- provide continuity in the event of a disaster
- meet legislative and regulatory requirements
- protect the interests of employees, clients and stakeholders”

Again, the Keeper fully agrees this statement.

The *RMP* is accompanied by a separate letter from the NES SIRO (see element 1) in which he states that: “We aim to use the information created by or entrusted to us in efficient and cost-effective ways that enable the development of a skilled and sustainable workforce and excellence in health and care for the people of Scotland. Achieving this would be impossible without good records management that operates with efficiency, transparency and accountability.”

NES discuss their objectives, the pursuance of which will be enhanced by robust records management, in their published Information Strategy:

[Corporate Strategy 2023-26 | NHS Education for Scotland \(nes.digital\)](#)

Key Group: The NES Information Governance & Security Business Unit, are responsible for ensuring that the *RMP* is appropriately implemented and that records management systems and processes are developed and monitored. They represent the first point of contact for “any incident that places patient confidentiality or the confidentiality, security, integrity or availability of NES information at risk” (*Information Governance Policy* (see element 3) page 10)

They are also responsible for reviewing relevant NES policy and guidance documents such as the *Data Cleansing Guidelines* (see element 6)

Local Records Management: Under the terms of the formal *Records Management Policy* (see element 3), NES Directors are required to nominate a representative, who will liaise with Information Governance & Security on the management of records in that directorate and contribute to the development of guidance and standards (*Policy* page 6).

Separately, public records in each service area are assigned an Information Asset Owner (IAO). These IAOs are recorded in a central *Information Asset Register*. A sample of this, very detailed, document has been provided to the Keeper together with a sample of a 'tracker' showing how the register is monitored by the information governance team (see element 4). This is a requirement of the *Information Security* and *Information Security Acceptable Use* policies (see element 8).

Information Asset Owners have the following responsibilities:

- Ensuring that systems under their authority have appropriate security policies in place;
- Ensuring that staff with access to the systems under their authority are aware of their responsibilities for maintaining the integrity of those systems;
- Ensuring that any contracts, service level agreements or other outsourcing arrangements with third parties to provide systems or services affecting the asset contain appropriate information governance clauses and instructions;
- Providing assurance to the Senior Information Risk Owner (SIRO) [see element 1] regarding the management of information risk affecting their information asset(s);
- Advising the Information Governance & Security Lead of significant changes to the information systems and assets under their authority." (*Information Security Policy* – see element 8 – page 8)

Each Director is responsible for 'orphan' records, which appear to have no owner (for example the person who created the record set has since left NES), are correctly managed by ensuring that they are allocated an Information Asset Owner. "Managers must notify the Digital Directorate in a timely manner of changes to staff personnel so that digital access can be provided and withdrawn in a controlled and auditable manner" (*Information Security Policy* – page 8).

Local Managers should also be able to provide advice on documents that may be classed a short-term value or of minor importance and that they can be destroyed outwith formal retention schedules.

6. Keeper's Summary

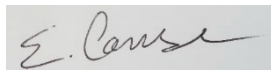
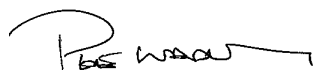
Elements **1 - 15** that the Keeper considers should be in a public authority records management plan have been properly considered by **NHS Education for Scotland**. Policies and governance structures are in place to implement the actions required by the plan.

7. Keeper's Determination

Based on the assessment process detailed above, the Keeper agrees the RMP of **NHS Education for Scotland**.

- The Keeper recommends that NHS Education for Scotland 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,



.....
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 **NHS Education for Scotland**. In agreeing this RMP, the Keeper expects *NHS Education for Scotland* to fully implement the agreed RMP and meet its obligations under the Act.



.....

Laura Mitchell
Deputy Keeper of the Records of Scotland