Records Management Plan

Document Control

Title	Records Management Plan
Author	Records Management Project Manager
Version Number	2.0
Review frequency	Annually
Next review date	May 2019

Version Control

Version	Date	Status	Prepared by	Amendments
0.1	21/04/2016	Draft	A Sharp	Initial draft – to project team
0.2	05/05/2016	Draft	D Paris	Updated with comments
0.3	08/12/2016	Draft	A Sharp	Updated with evidence / comments
0.4	13/01/2017	Draft	A Sharp	Updated with evidence / comments
0.5	20/02/2017	Draft	A Sharp	Revisions
0.6	21/02/2017	Draft	A Sharp	Revisions
0.7	22/02/2017	Draft	A Sharp	Revisions
0.8	08/03/2017	Draft	A Sharp	Revisions
0.9	13/03/2017	Draft	A Sharp	Revisions
0.10	20/03/2017	Draft	A Sharp	Revisions
1.0	27/06/2017	Final	D Paris	Approved by SMT
1.1	18/04/2018	Draft	D Paris	Amendments in response to NRS Interim Report
2.0	27/04/18	Final	D Steel	Approved

The Keeper of the Records of Scotland will be alerted to any changes that are made to this Records Management Plan in accordance with section 5(6) of the Public Records (Scotland) Act 2011

CONTENTS

HISTORIC ENVIRONMENT SCOTLAND RECORDS MANAGEMENT PLAN

COVERING STATEMENT

I am pleased to submit Historic Environment Scotland's records management plan for assessment by the Keeper of the Records of Scotland.

Historic Environment Scotland (HES) is a new organisation, which took up its full statutory role on the 1 October 2015, created by the merger of Historic Scotland (HS) and the Royal Commission on the Ancient and Historical Monuments (RCAHMS). HES is responsible for more than 300 properties of national importance including Edinburgh Castle, Neolithic Orkney, Fort George and numerous smaller sites, drawing more than 3 million visitors per year. Other responsibilities include curation of internationally significant collections including over five million drawings, photographs, negatives and manuscripts, along with 20 million aerial images of locations across the world

The HES Records Management Plan outlines the current position of records management within HES with proposed actions for improvement. It is important to recognise that records management in HES is in the early stages of considerable change. Over the next few years HES records management policies, processes and procedures will be developed and implemented, staff will be trained and the culture of information management will be introduced and fostered. This is the start of a journey which will see many improvements over the coming years.

In 2014, a team from HS started a project with the purpose of reviewing the effectiveness of records management in HS and RCAHMS and producing the first records management plan, strategy and policy for HES. The team carried out an information audit which concluded that across both organisations there were pockets of good recordkeeping being undertaken, however, in most cases staff did not fully appreciate the rationale behind good recordkeeping, too much information was retained beyond its usefulness, legal requirement or business need. It also noted a lack of corporate policies and procedures across both organisations and no dedicated records management governance structure was in place.

As a result of this review, HES has put the following in place:

- Identification of a Director to have strategic accountability for records management;

- Appointment of a senior manager as Head of Information Governance to have day-to-day operational responsibility for records management;

- Extended the remit of the project team to produce and implement the records management plan.

We recognise there is still much work to do. Our records management plan is forward looking and incorporates an ambitious programme which will move us beyond compliance to best practice in the coming years.   During implementation of the plan, we will deliver comprehensive training on records management and information governance to all staff, and we will embark on a project to select and implement a system for managing electronic records, which is capable of both supporting our business processes and maintaining an accurate audit trail of the records we create.

ALEX PATERSON
Chief Executive

ELEMENT 1: SENIOR MANAGEMENT RESPONSIBILITY
Identify an individual at senior level who has overall strategic accountability for records management.

Introduction	Section 1(2)(a)(i) of the Act specifically requires a RMP to identify the individual responsible for the management of the authority's public records. An authority's RMP must name and provide the job title of the senior manager who accepts overall responsibility for the RMP that has been submitted. It is vital that the RMP submitted by an authority has the approval and support of that authority's senior management team. Where an authority has already appointed a Senior Information Risk Owner, or similar person, they should consider making that person responsible for the records management programme. It is essential that the authority identifies and seeks the agreement of a senior post-holder to take overall responsibility for records management. That person is unlikely to have a day-to-day role in implementing the RMP, although they are not prohibited from doing so. As evidence, the RMP could include, for example, a covering letter signed by the senior post-holder. In this letter the responsible person named should indicate that they endorse the authority's record management policy (See Element 3). Read further explanation and guidance about element 1 - http://www.nas.gov.uk/recordKeeping/PRSA/guidanceElement1.asp
Statement of Compliance	Donella Steel, Director of Finance and Performance, has senior responsibility for all aspects of Records Management in HES, and is the corporate owner of the HES Records Management Plan. Donella Steel is also the Senior Information Risk Owner (SIRO) for HES.
Evidence of Compliance	Evidence to be submitted in support of Element 1 includes:
	Completed and approved Records Management Strategy Records Management Policy Formal Appointment letter for SIRO including job description & SIRO Handbook Covering letter from Chief Executive Statement of Responsibility for Records Management Information Management Strategy – Corporate Information Extracts from Information Assurance Maturity Model Reporting Template
Future Developments	There are no planned future developments in respect of Element 1. If Senior Management Responsibility changed, however, policies and procedures would need to be examined in the light of these changes. We will continue to develop the information risk and the records management culture within the organisation. This will be driven by the Information Governance Team along with the Information Asset Owner Network and the Information Asset Register which, in turn, will feed into the Information Assurance Maturity Model.
Assessment and Review	This element will be reviewed as soon as there any changes in personnel.
Responsible Officer(s)	Donella Steel, Director of Finance and Performance

ELEMENT 2: RECORDS MANAGER RESPONSIBILITY

Identify an individual within the authority, answerable to senior management, to have day-to-day operational responsibility for records management within the authority.

Introduction	Section 1(2) (a)(ii) of the Act specifically requires a RMP to identify the individual responsible for ensuring the authority complies with its plan. An authority's RMP must name and provide the job title of the person responsible for the day-to-day operation of activities described in the elements in the authority's RMP. This person should be the Keeper's initial point of contact for records management issues. It is essential that an individual has overall day-to-day responsibility for the implementation of an authority's RMP. There may already be a designated person who carries out this role. If not, the authority will need to make an appointment. As with element 1 above, the RMP must name an individual rather than simply a job title. It should be noted that staff changes will not invalidate any submitted plan provided that the all records management responsibilities are transferred to the incoming post holder and relevant training is undertaken. This individual might not work directly for the scheduled authority. It is possible that an authority may contract out their records management service. If this is the case an authority may not be in a position to provide the name of those responsible for the day-to-day operation of this element. The authority must give details of the arrangements in place and name the body appointed to carry out the records management function on its behalf. It may be the case that an authority's records management programme has been developed by a third party. It is the person operating the programme on a day-to-day basis whose name should be submitted. Read further explanation and guidance about element 2 - http://www.nas.gov.uk/recordKeeping/PRSA/guidanceElement2.asp
Statement of Compliance	David Paris, Head of Information Governance, has responsibility for day-to-day implementation of all HES records management activities described in the HES Records Management Plan. David Paris owns all the actions identified in the future developments section of this document. It should be noted that the role of Head of Records Management has changed significantly since it was first advertised in 2015. The role has now become the Head of Information Governance and now encompasses Freedom of Information and Information Security.
Evidence of Compliance	Evidence to be submitted in support of Element 2 includes:
	Completed and approved Records Management Policy Head of Records Management Person Specification Head of Records Management Job Advert ICO Registration Records Management Strategy Statement of Responsibility for Records Management Information Management Strategy Records Management Project PID Information Assurance Board ToR Extract from Information Assurance Maturity Model Reporting Template
Future Developments	

	There are no planned future developments in respect of Element 2. However, if the Records Management responsibility changed, policies and procedures would need to be examined in the light of these changes.
	The previous reporting mechanism for the IG Team was the Information and Information Systems Governance Board (IISGB). The focus for this group was however the migration to the HES network, although there was reporting on the progress of the RMP. This Board has now disbanded and the Head of Information Governance has instigated the Information Assurance Board who report into the Audit, Risk and Assurance Committee and whose remit is to oversee the information governance processes, systems and practice across HES.
	The IAO Network has been initiated and implementation is progressing in line with the production of the IAR.
Assessment and Review	This element will be reviewed as soon as there any changes in personnel.
Responsible Officer(s)	David Paris, Head of Information Governance.

ELEMENT 3: RECORDS MANAGEMENT POLICY STATEMENT

A records management policy statement underpins effective management of an authority's records and information. It demonstrates to employees and stakeholders that managing records is important to the authority and serves as a mandate for the activities of the records manager.

Introduction	The Keeper expects each authority's plan to include a records management policy statement. The policy statement should describe how the authority creates and manages authentic, reliable and useable records, capable of supporting business functions and activities for as long as they are required. The policy statement should be made available to all staff, at all levels in the authority. The statement will properly reflect the business functions of the public authority. The Keeper will expect authorities with a wide range of functions operating in a complex legislative environment to develop a fuller statement than a smaller authority. The records management statement should define the legislative, regulatory and best practice framework, within which the authority operates and give an overview of the records management processes and systems within the authority and describe how these support the authority in carrying out its business effectively. For electronic records the statement should describe how metadata is created and maintained. It should be clear that the authority understands what is required to operate an effective records management system which embraces records in all formats. The records management statement should include a description of the mechanism for records management issues being disseminated through the authority and confirmation that regular reporting on these issues is made to the main governance bodies. The statement should have senior management approval and evidence, such as a minute of the management board recording its approval, submitted to the Keeper. The other elements in the RMP, listed below, will help provide the Keeper with evidence that the authority is fulfilling its policy. Read further explanation and guidance about element 3 – http://www.nas.gov.uk/recordKeeping/PRSA/guidanceElement3.asp
Statement of Compliance	Historic Environment Scotland is committed to a systematic and planned approach to the management of records within the organisation, from their creation to their ultimate disposal or archive. This approach will ensure that Historic Environment Scotland can: • Control the quality, quantity and security of the information that it generates; and • Maintain the information in an effective manner whilst ensuring compliance with legislative requirements A Records Management Policy Statement, reflective of the current and future record keeping arrangements in Historic Environment Scotland has been developed. This Policy Statement has been approved by the Senior Information Risk Owner in Historic Environment Scotland and the Information and Information Systems Governance Board.
Evidence of Compliance	Evidence to be submitted in support of Element 3 includes:
	Completed and approved Records Management Policy Records Management Strategy SMT Minutes Information Management Strategy

	Information Assurance Board ToR
Future Developments	HES must put in place a process for ensuring that all policies and procedures for the organisation remain relevant and up to date. To ensure that this occurs, we will design an Approval Log setting out when policies / guidance are due to be reviewed and appoint an owner whose role will be to ensure that the policies / guidance are reviewed, updated and approved where appropriate. The Head of Information Governance will ensure that all policies and procedures are reviewed formally in conjunction with business areas where appropriate on an annual basis. The IAO Network has been established and is progressing. This will assist the IG Team in ensuring that business area interests are fully represented in any policy / procedure change. A report will then be provided for the Information Assurance Board and where appropriate, SMT.
Assessment and Review	The Joint Senior Management Team and the Information and Information Systems Governance Board have approved the Records Management Policy. The Records Management Policy will be communicated to all staff and will be reviewed annually by the Head of Information Governance.
Responsible Officer(s)	David Paris, Head of Information Governance.

ELEMENT 4: BUSINESS CLASSIFICATION

A business classification scheme describes what business activities the authority undertakes – whether alone or in partnership.

Introduction	The Keeper expects an authority to have properly considered business classification mechanisms and its RMP should therefore reflect the functions of the authority by means of a business classification scheme or similar. A business classification scheme usually takes the form of a hierarchical model or structure diagram. It records, at a given point in time, the informational assets the business creates and maintains, and in which function or service area they are held. As authorities change the scheme should be regularly reviewed and updated. A business classification scheme allows an authority to map its functions and provides a structure for operating a disposal schedule effectively. Some authorities will have completed this exercise already, but others may not. Creating the first business classification scheme can be a time-consuming process, particularly if an authority is complex, as it involves an information audit to be undertaken. It will necessarily involve the cooperation and collaboration of several colleagues and management within the authority, but without it the authority cannot show that it has a full understanding or effective control of the information it keeps. Although each authority is managed uniquely there is an opportunity for colleagues, particularly within the same sector, to share knowledge and experience to prevent duplication of effort. All of the records an authority creates should be managed within a single business classification scheme, even if it is using more than one record system to manage its records. An authority will need to demonstrate that its business classification scheme can be applied to the record systems which it operates. Read further explanation and guidance about element 4 - http://www.nas.gov.uk/recordKeeping/PRSA/guidanceElement4.asp.
Statement of Compliance	HES recognises the importance and benefits of organising its information in such a way that facilitates customer service, business efficiency and information management. Throughout 2013/14, an information audit exercise was completed alongside representatives from all business areas. The Information Governance Team worked with the business areas to identify the organisation's core functions, component activities and associated transactions in order to develop a comprehensive file plan for HES. These were submitted to and approved by the relevant Director. As part of the exercise it was discovered that the current shared drive(s) had been largely uncontrolled and had grown organically over many years. This resulted in some file paths reaching 14 levels deep. In addition, we will be moving to an eDRMS in the next 1–3 years and as such, such an upheaval to implement the BCS wholesale in the current structure would be counter-productive for the organisation. The BCS is however being used as part of the IAR work that is being undertaken and some business areas have chosen to implement aspects of the BCS.

Evidence of Compliance	Evidence to be submitted in support of Element 4 includes:
	Completed and approved Information Audit Report HES Business Classification Scheme RecordPoint Contract Records Management Policy eDRMS Options Report Information Assurance Board ToR
Future Developments	Approval has been given for the purchase and implementation of an electronic document records management system (eDRMS). Some initial work in scoping out the project has been undertaken with consultants. A contract has been awarded to RecordPoint to supply the Records Management module which will initially be implemented across the existing HES file shares. Work is progressing in completing the business case to develop SharePoint as Document Management and information hub and this will be submitted as evidence once complete. In the interim, the IG Team will start to work with business areas to re-build their shared network drive structure, where appropriate, along the lines of the agreed file plans although the technical solutions to support this will be limited. eDRMS is likely to be introduced in the next 1-3 years which will include information from the file plans and based on the new BCS and RRS which be validated with the business prior to implementation. Full scope notes for the BCS are in progress.
Assessment and Review	During implementation of the eDRMS the IG Team will work with the business areas to review the BCS and RRS to ensure that they remain fit for purpose and are amended / updated accordingly.
Responsible Officer(s)	David Paris, Head of Information Governance.

ELEMENT 5: RETENTION SCHEDULES

A retention schedule is a list of records for which pre-determined disposal dates have been established.

Introduction	Section 1(2) (b)(iii) of the Act specifically requires a RMP to include provision about the archiving and destruction or other disposal of the authority's public records. An authority's RMP must demonstrate the existence of and adherence to corporate records retention procedures. The procedures should incorporate retention schedules and should detail the procedures that the authority follows to ensure records are routinely assigned disposal dates, that they are subsequently destroyed by a secure mechanism (see element 6) at the appropriate time, or preserved permanently by transfer to an approved repository or digital preservation programme (See element 7). The principal reasons for creating retention schedules are: • to ensure records are kept for as long as they are needed and then disposed of appropriately • to ensure all legitimate considerations and future uses are considered in reaching the final decision. • to provide clarity as to which records are still held by an authority and which have been deliberately destroyed. "Disposal" in this context does not necessarily mean destruction. It includes any action taken at the agreed disposal or review date including migration to another format and transfer to a permanent archive. A retention schedule is an important tool for proper records management. Authorities who do not yet have a full retention schedule in place should show evidence that the importance of such a schedule is acknowledged by the senior person responsible for records management in an authority (see element 1). This might be done as part of the policy document (element 3). It should also be made clear that the authority has a retention schedule in development. An authority's RMP must demonstrate the principle that retention rules are consistently applied across all of an authority's record systems. Read further explanation and guidance about element 5 - http://www.nas.gov.uk/recordKeeping/PRSA/guidanceElement5.asp
Statement of Compliance	HES Records Retention Schedules have been prepared by working with the business areas. In some areas retention policies already existed – e.g. HR and Finance; but these needed further reviewing and further developed to become more effective. In other areas there were no clear records retention policies – e.g. Communications and IT and these have now been developed. HES will continue to work with the business areas to further develop and implement currently agreed Records Retention Schedule and Policies based on the key record types held by the organisation – both paper and electronic. Recommended minimum retention periods have been defined in line with statutory and legislative obligations and business needs. The retention schedules have been published on the staff Intranet

Evidence of Compliance	Evidence to be submitted in support of Element 5 includes:
	Completed and approved Retention and Disposal Schedule(s) Information Audit Report Director approval of Retention and Disposal Schedule(s) Publication of Retention Schedules Information Asset Register Hand-outs, Templates, Business Case and Screenshots Extract from Information Assurance Maturity Model Reporting Template

Future Developments	The Information Governance Team will work with management and staff throughout HES to further develop individual business area's Records Retention Schedules.
	
	Further work will be undertaken to ensure that
	   – the retention schedules remain fit for purpose particularly following the creation of Historic Environment Scotland Enterprises (HESe). HESe is the trading arm of HES and is a wholly owned subsidiary.
	   – The published retention schedules are reviewed and up to date.
	   – A comprehensive training programme covering the benefits of records management including retention and disposal will be developed.
	
	The agreed Retention and Disposal Schedule(s) will apply to both physical and digital records.
	
	The current IMPReS system used to track physical files is no longer supported by the vendor and we will look to migrate the data from this system to allow us to mmanage physical and hybrid records along with electronic records in SharePoint all in the one interface.
	
	Approval in principle has been given by senior management for the purchase and implementation of an electronic document records management system (eDRMS). The retention periods defined in the agreed Retention and Disposal Schedule(s) will be used in the implementation of the chosen eDRMS.
	
	In the interim, the schedules will remain on the staff intranet and will act as a vital reference point for all staff when assessing how long they need to retain business information.
	
	Work has commenced within HES to implement an Information Asset Register which includes the purchase of specialist software which will allow us to capture data but with significantly more scope for utilising the information following its capture. This project is in its infancy but as it progresses, it will be rolled out across the organisation.
	
	IAO's within the business areas are the first point of contact on any retention issue for their particular part of the business.

Assessment and Review	The Head of Information Governance along with IAO's will be responsible for monitoring and reviewing the schedules ensuring that they continue to reflect recordkeeping best practice as well as legal and statutory obligations. An informal review of the Retention Schedule(s) will be undertaken locally by IAO's. A formal review will be undertaken by the Information Governance Team annually.

	Any changing requirements will be assessed and approved by the Information Governance Team before implementing. The Retention Schedules will be amended and updated.
Responsible Officer(s)	David Paris, Head of Information Governance.

ELEMENT 6: DESTRUCTION ARRANGEMENTS

It is not always cost-effective or practical for an authority to securely destroy records in-house. Many authorities engage a contractor to destroy records and ensure the process is supervised and documented.

Introduction	Section 1(2) (b)(iii) of the Act specifically requires a RMP to include provision about the archiving and destruction, or other disposal, of an authority's public records.
	An authority's RMP must demonstrate that proper destruction arrangements are in place.
	A retention schedule, on its own, will not be considered adequate proof of disposal for the Keeper to agree a RMP. It must be linked with details of an authority's destruction arrangements. These should demonstrate security precautions appropriate to the sensitivity of the records. Disposal arrangements must also ensure that all copies of a record – wherever stored – are identified and destroyed.
	Read further explanation and guidance about element 6 - http://www.nas.gov.uk/recordKeeping/PRSA/guidanceElement6.asp
Statement of Compliance	HES staff are required to dispose of paper documents in line with published guidance. Most HES offices have confidential waste bins or access to confidential waste facilities that are specifically for the secure disposal of information assets.
	For large volume shredding HES uses Shred-It to carry out on-site shredding http://www.shredit.co.uk.
	HES has 2 temporary, rented offsite physical storage facilities. The Records Management Team are working with the business areas to close these down and find alternative accommodation within the HES estate.
	HES has contracted with RecordPoint to supply the Records Management facility of the eDRMS in progress. RecordPoint will give HES the ability apply retention policies and record the creation and deletion of the records held on the shared drives.
	The current contract for on-site shredding is sub-contracted via our Facilities Management Contract is contracted, via Records Management, to Shred-it
	The Registry Team keeps records of all files that are open, closed, destroyed or transferred to NRS for archiving.
	Previously all Historic Scotland IT equipment belonged to The Scottish Government and their IT team dealt with the disposal of IT equipment. Following the move to our own IT Network, there may be some legacy hardware belonging to The Scottish Government. In those cases, Scottish Government will be given first refusal for disposing of that equipment.
	RCAHMS had their own equipment and methods of destruction.
Evidence of Compliance	Evidence to be submitted in support of Element 6 includes:
	Completed and approved Retention and Disposal Schedules

	Retention and Disposal Guidance Shred-it Proposal for on-site shredding Sample Shred-it Customer Service Agreement RecordPoint Contract HES Back-up Strategy Gap Analysis Information Security Roadmap Registry Project PID Extract from IMPReS Signed Shred-it Service Agreement
Future Developments	The disposal of physical and digital records will be clearly communicated to all staff as part of the Information Management Training. The management of confidential waste can be further by procuring and supplying cross-cut shredders to those outlying areas with little information or access to Shred-it contract.. We will also undertake audits to ensure confidential waste is being disposed of correctly. HES's Information Security Manager is working towards bringing the orgainisation in compliance with ISO:27001 and the Information Security Management System. HES is now responsible for its own IT equipment following the move from the previous arrangements. We will continue to access the contract that was in place with RCAHMS prior to the merger but will ensure that the secure destruction of IT equipment is included (or be available) in any contract awarded.
Assessment and Review	The destruction arrangements will be reviewed formally each year by the Head of Information Governance in conjunction with the Head of IT and a report provided to SMT.
Responsible Officer(s)	David Paris, Head of Information Governance. Edgar Dodds, Head of IT

ELEMENT 7: ARCHIVING AND TRANSFER ARRANGEMENTS

This is the mechanism by which an authority transfers records of enduring value to an appropriate archive repository, specifying the timing of transfers and other terms and conditions.

Introduction	Section 1(2)(b)(iii) of the Act specifically requires a RMP to make provision about the archiving and destruction, or other disposal, of an authority's public records. An authority's RMP must detail its archiving and transfer arrangements and ensure that records of enduring value are deposited in an appropriate archive repository. The RMP will detail how custody of the records will transfer from the operational side of the authority to either an in-house archive, if that facility exists, or another suitable repository, which must be named. The person responsible for the archive should also be cited. Some records continue to have value beyond their active business use and may be selected for permanent preservation. The authority's RMP must show that it has a mechanism in place for dealing with records identified as being suitable for permanent preservation. This mechanism will be informed by the authority's retention schedule which should identify records of enduring corporate and legal value. An authority should also consider how records of historical, cultural and research value will be identified if this has not already been done in the retention schedule. The format/media in which they are to be permanently maintained should be noted as this will determine the appropriate management regime. Read further explanation and guidance about element 7-http://www.nas.gov.uk/recordKeeping/PRSA/guidanceElement7.asp
Statement of Compliance	HES currently works with the National Records of Scotland (NRS) for permanent preservation of HES records. HES records identified as being of historical interest are transferred to the National Records of Scotland for permanent preservation. HES and NRS have now developed a digital means of requesting and receiveing file retransmissions. This will ensure the continuing preservation of the NRS archive whilst allowing HES to access the information held by NRS.
Evidence of Compliance	Evidence to be submitted in support of Element 7 includes:
	Completed and approved Retention and Disposal Schedule Archiving and Transfer Arrangements Statement Retention and Disposal Guidance Information Management Strategy – Corporate Information eDRMS Business Case (to be submitted once complete) Data Protection Code of Practice – Archive Collections
Future Developments	Current archiving arrangements with NRS for former Historic Scotland files will continue for the time-being as will archiving for the former RCAHMS National Collection.

	Verbal confirmation is in place and NRS are drafting a Service Level Agreement. HES is currently in discussion with the Client Management Team in NRS regarding archiving and transfer arrangements with a view to signing an appropriate Memorandum of Understanding. The NRS Client Management Team have indicated that they are not in a position to do this until after 25th May 2018. Work will however need to be undertaken to ensure that there is a consistent set policies and procedures in place that will ensure a consistent approach for the transfer and/or archive of records taking into account legislation such as Freedom of Information (Scotland) Act 2002 and the Data Protection Act 1998/General Data Protection Regulation.
Assessment and Review	Archive and Transfer Arrangements will be reviewed alongside the processes and procedures written. All future developments will include a statement on assessment and review cycles.
Responsible Officer(s)	David Paris, Head of Information Governance. Lesley Ferguson, Head of Archives and Engagement

ELEMENT 8: INFORMATION SECURITY

Information security is the process by which an authority protects its records and ensures they remain available. It is the means by which an authority guards against unauthorised access and provides for the integrity of the records. Robust information security measures are an acknowledgement that records represent a risk as well as an asset. A public authority should have procedures in place to assess and contain that risk.

Introduction	Section 1(2) (b)(ii) of the Act specifically requires a RMP to make provision about the archiving and destruction or other disposal of the authority's public records. An authority's RMP must make provision for the proper level of security for its public records. All public authorities produce records that are sensitive. An authority's RMP must therefore include evidence that the authority has procedures in place to adequately protect its records. Information security procedures would normally acknowledge data protection and freedom of information obligations as well as any specific legislation or regulatory framework that may apply to the retention and security of records. The security procedures must put in place adequate controls to prevent unauthorised access, destruction, alteration or removal of records. The procedures will allocate information security responsibilities within the authority to ensure organisational accountability and will also outline the mechanism by which appropriate security classifications are linked to its business classification scheme. Read further explanation and guidance about element 8 - http://www.nas.gov.uk/recordKeeping/PRSA/guidanceElement8.asp
Statement of Compliance	HES has developed a range of information security policies and procedures which have been published and all staff are required to comply with these. The policies have been approved by the Information and Information Security Governance Board (IISGB) and are to be reviewed on an annual basis. HES has an Information Security Manager whose role is to ensure that Information Security policies are complied with and any breaches are reported promptly to the SIRO and Information Assurance Board. However the current remit only includes digital information. Information Security and Information Assurance in HES is organised in line with the guidance and requirements in the HMG Standards; namely the Security Policy Framework, the CESG IA Standards and Good Practice Guides. All these standards are closely aligned to the International Security standard, ISO27001. As a minimum requirement all staff are subject to recruitment controls known as the Baseline Personnel Security Standard (BPSS). The purpose of personnel security procedures is to provide a level of assurance as to the trustworthiness, integrity and reliability of all HES employees, contractors and temporary staff. HES has introduced bespoke eLearning courses containing an introduction to data protection as well as information security. Staff who come into contact or who manage staff who come into contact with personal data have been invited to attend a mandatory ½ day training session on the Data Protection Act 1998.

Evidence of Compliance	Evidence to be submitted in support of Element 8 includes:
	Completed and approved Data Protection Policy (GDPR) Surveillance Camera Code of Practice Information Management Strategy Information Security Policy Security Incident Reporting Policy Protocol Policy System Policy suite Communication on Protocol Policy System ½ day Data Protection Training (inc handouts) eLearning DPA and Information Security course information Example GDPR Privacy Policy Data Processing Agreement ISO:27001 Gap Analysis Information Security Roadmap Extract from Information Assurance Maturity Model Reporting Template
Future Developments	In 2016 the then IT Security Officer published a suite of policies and procedures. However these were purely based around IT security and the protection of digital information. The Head of Information Governance has appointed an external contractor who has provided an interactive system for IT and Information Security policies based on ISO 27000, legislation and best practice. This has been approved by SMT and the IG Team are moving to implementation in the organisation. These will then be published on the Intranet and staff will be made aware of their existence. The Information Security Manager has recently completed a Gap Analysis of the current security position in line with ISO:27001 which has allowed HES to baseline and assess its information security maturity. This has highlighted a number of weaknesses which the organisation will look to address in the coming months. Initiatives either started or in the early stages of development are: • Corporate Risk Policy and Strategy (April 2017) • Information Security Classification Guidance (drafted but on hold) • Sending Information Guidance (drafted but on hold) • FoI Training • Risk Analysis and Management Policy (ISO:27001) • Information Risk Analysis Processes and Guidance (ISO:27001)
Assessment and Review	The Information Security policies should be informally reviewed by the Information Security Manager and the Head of Information Governance bi-annually and formally at least annually by the Information Assurance Board with a report to the SMT confirming they continue to meet requirements.
Responsible Officer(s)	David Paris, Head of Information Governance Donella Steel, Director of Finance and Performance Edgar Dodds, Head of IT [ ] Information Security Manager

ELEMENT 9: DATA PROTECTION

An authority that handles personal information about individuals has a number of legal obligations to protect that information under the Data Protection Act 1998.

Introduction	The Keeper will expect an authority's RMP to indicate compliance with its data protection obligations. This might be a high level statement of public responsibility and fair processing. If an authority holds and process information about stakeholders, clients, employees or suppliers, it is legally obliged to protect that information. Under the Data Protection Act, an authority must only collect information needed for a specific business purpose, it must keep it secure and ensure it remains relevant and up to date. The authority must also only hold as much information as is needed for business purposes and only for as long as it is needed. The person who is the subject of the information must be afforded access to it on request. Read further explanation and guidance about element 9 - http://www.nas.gov.uk/recordKeeping/PRSA/guidanceElement9.asp
Statement of Compliance	HES has a range of policies and procedures in place to ensure that personal data is managed securely in accordance with the Data Protection Act and the forthcoming General Data Protection Regulation. The Head of Information Governance is in overall charge of Data Protection within HES and is the Data Protection Officer. HES has an approved Data Protection Policy (GDPR) which is published internally and externally. The Information Manager holds the Data Protection Practitioner Certificate. HES's registration number in the Data Protection Register is ZA143443.
Evidence of Compliance	Evidence to be submitted in support of Element 9 includes:
	Completed and Approved ICO Registration Data Protection Policy (GDPR) Internal Scheme of Delegations (revised) Privacy Compliance Templates Privacy Compliance Guidance Data Processing Agreements (revised) ½ day Data Protection Training (inc handouts) eLearning Data Protection Training (revised) FoI / DPA Combined Action Plan Data Protection Code of Practice – Archive Collections Surveillance Systems Code of Practice Subject Access Request Policy (revised) Extract from Information Assurance Maturity Model Reporting Template GDPR Readiness Report SGIA GDPR Arrangements GDPR Plan

Future Developments	HES will continue to provide comprehensive training and awareness for all staff in order to ensure that they are aware of their responsibilities in managing, processing and protecting personal data. The Information Manager will develop a data sharing statement and will undertake an audit to determine who HES shares data with and that the necessary agreements are in place. As mentioned earlier, we will appoint IAO's within the business areas. Part of their role will be ensure that they are the first point of contact for any data / information sharing within their particular part of the business and ensuring that the Information Manager is fully aware.
Assessment and Review	The policies and codes of practice will be reviewed by the Head of Information Governance and the Information Manager ensuring they remain accurate and up to date. All amendments to the Data Protection Policy are required to be approved by the HES Board, who hold ultimate responsibility for Data Protection in HES. The register entry will be regularly monitored and updated as necessary.
Responsible Officer(s)	David Paris, Head of Information Governance Roger Green, Information Manager

ELEMENT 10: BUSINESS CONTINUITY AND VITAL RECORDS
A business continuity and vital records plan serves as the main resource for the preparation for, response to, and recovery from, an emergency that might affect any number of crucial functions in an authority.

Introduction	The Keeper will expect an authority's RMP to indicate arrangements in support of records vital to business continuity. Certain records held by authorities are vital to their function. These might include insurance details, current contract information, master personnel files, case files, etc. The RMP will support reasonable procedures for these records to be accessible in the event of an emergency affecting their premises or systems. Authorities should therefore have appropriate business continuity plans ensuring that the critical business activities referred to in their vital records will be able to continue in the event of a disaster. How each authority does this is for them to determine in light of their business needs, but the plan should point to it. Read further explanation and guidance about element 10 - http://www.nas.gov.uk/recordKeeping/PRSA/guidanceElement10.asp
Statement of Compliance	This is an area that needs development. HES business areas have individual business continuity/emergency plans and site response plans in place. There is a major incident plan for both the former HS and RCAHMS which were approved by the former Chief Executives. However, all plans require to be updated following the creation of HES and the change of IT systems. HES has an on-call protocol which sets out how the organisation should respond to emergencies. The on-call protocol identifies a Senior On-Call Officer who is a member of the Senior Management Team. They are the first point of contact for each on-call period and are able to advise relevant site staff on appropriate actions and, where necessary, to authorise activation of the organisation's Emergency Response Arrangements. The work being undertaken on the Information Asset Register will allow business areas to identify and record their vital records and the potential risks to that information, systems and collections. A Business Impact Assessment for Registry covering the paper records has been completed and approved.
Evidence of Compliance	Evidence to be submitted in support of Element 10 includes: **Completed and Approved** Retention and Disposal Schedule Information Asset Register Hand-outs, Templates, Business Case and Screenshots BIA for the HES Registry Example BCP for Archives

Future Developments	HES requires a comprehensive business continuity strategy and improvement plan to review all existing procedures and build a comprehensive network of roles and responsibilities in the event of an emergency. The SMT need to take ownership of this and ensure that business continuity within HES is taken forward and improved. The Business Impact Assessment for the Registry function has now been completed and approved and work will commence to complete a Business Continuity Plan but this will depend on the direction Business Continuity within HES takes. Business areas will be required to identify and document their vital records and the potential risks to information, systems and collections. This information will be recorded on the information asset register. All existing plans and procedures should be updated during 2017/18 to reflect the new organisation and the new IT structure.
Assessment and Review	All Business Continuity Plans and Site Emergency Plans will be tested at least annually.
Responsible Officer(s)	David Paris, Head of Information Governance for Vital Records only Peter McGrath, Head of Physical Security for Business Continuity Project

ELEMENT 11: AUDIT TRAIL

An audit trail is a sequence of steps documenting the movement and/or editing of a record resulting from activities by individuals, systems or other entities.

Introduction	The Keeper will expect an authority's RMP to provide evidence that the authority maintains a complete and accurate representation of all changes that occur in relation to a particular record. For the purpose of this plan 'changes' can be taken to include movement of a record even if the information content is unaffected. Audit trail information must be kept for at least as long as the record to which it relates. This audit trail can be held separately from or as an integral part of the record. It may be generated automatically, or it may be created manually. Read further explanation and guidance about element 11 - http://www.nas.gov.uk/recordKeeping/PRSA/guidanceElement11.asp
Statement of Compliance	This is an area that needs development. Currently, the Registry Team at Longmore House are able to track the creation, destruction and transfer to archive of all paper files. A Records Management Manual written in 2012 exists and it is out of date but, the principles of how to manage paper records will still apply. There is no registry function for John Sinclair House. The majority of records are held electronically on shared network drives with no audit facility. Following the move to the HES IT Network, there has been a lock-down of permissions on the shared network drives which means that that the ability for users to add folders has been removed. This move allows the Information Governance Team (IGT) to control the growth of folders and allows a more consistent approach to folder setup conventions. However, even with this step, there is no ability to implement an audit facility on the shared drives and staff are able to edit, rename, delete and hold multiple copies of files. Some of the separate IT systems in use within HES have an audit facility but at present, the majority of records in the electronic environment can be moved, edited, renamed and deleted without any of these actions being auditable. **HR and Finance** The records held by both of these functions are stored within drives which are only accessible to the relevant staff. Disposal of records takes place in accordance with the timescales set out in the approved retention schedule(s). HES is committed to improving the way in which electronic documents are managed throughout the organisation. Approval in principle has been granted for the procurement of an Electronic Records Management System (eDRMS). HES will select and implement a system in which records can be created and maintained with audit trail information. In the interim, HES will work to improve the management of electronic records within its current systems. Guidelines covering document naming, use of version control, and the management of email have been developed to support colleagues. Staff will be introduced to and trained in these rules and

	procedures in 2017/18 in order to improve how HES captures, stores, names and disposes of its records. All records will be managed using the agreed Retention and Disposal Schedule(s). RecordPoint contract has been awarded for the Records Management aspect of eDRMS. This includes the ability to manage physical files and will replace the current Registry system. This will allow HES to start to manage the records more effectively including auditing when information has been destroyed.
Evidence of Compliance	Evidence to be submitted in support of Element 11 includes:
	Completed and Approved Records Management Strategy RaisersEdge Audit Trail Manual Removal of permissions notice to all staff HM System Audit trail example(s) Extract from HM System User Manual Managing Email Guidance Vernon system audit descriptor Vernon Audit trail example SPECTRUM standard audit procedure (Collections) Naming Conventions for Electronic Records Guidance Draft Audit Reporting Policy for Integra eSeries2 Registry Project PID Extract from HR System Audit Report HR Audit Guidance Notes Extract from IMPReS RecordPoint Contract

Future Developments	HES is committed to improving the way in which electronic documents are managed throughout the organisation. HES will continure to develop its eDRMS capabilities. There is a business case in development to develop SharePoint as the Document Management aspect of eDRMS. SharePoint will become the single source of truth for all documents and information not stored in line of business systems. SharePoint will also fulfil the Intranet function again ensuring a single source of truth in HES.
	
	In the interim, HES will work to improve the management of electronic records within its current systems.
	   – Guidelines covering document naming, use of version control, and the management of email have been developed and published to support colleagues.
	   – Staff will be introduced to and trained in these rules and procedures in 2018/19 in order to improve how HES captures, stores, names and disposes of its records.
	   – All records will be managed using the agreed Retention and Disposal Schedule(s).
	
	HES is committed to implementing an eDRMS in the next 1 - 3 years.
	
	Audit for some HES systems is limited. For example, the HR system audit facility is over-complicated, is difficult to apply and has not been fully implemented. The HR system is however due for re-tender in the next 12

	months or so. The IG Team will insist on reviewing the tender specification to ensure that a full audit facility is available and that it is fit for purpose.
Assessment and Review	This element is currently under review. The Keeper of the Records of Scotland will be kept informed of progress and changes to this element.
Responsible Officer(s)	David Paris, Head of Information Governance. Donella Steel, Director of Finance and Performance and SIRO Edgar Dodds, Head of IT.

ELEMENT 12: COMPETENCY FRAMEWORK FOR RECORDS MANAGEMENT STAFF

A competency framework lists the core competencies and the key knowledge and skills required by a records manager. It can be used as a basis for developing job specifications, identifying training needs, and assessing performance

Introduction	The Keeper will expect an authority's RMP to detail a competency framework for person(s) designated as responsible for the day-to-day operation of activities described in the elements in the authority's RMP. It is important that authorities understand that records management is best implemented by a person or persons possessing the relevant skills. A competency framework outlining what the authority considers are the vital skills and experiences needed to carry out the task is an important part of any records management system. If the authority appoints an existing non-records professional member of staff to undertake this task, the framework will provide the beginnings of a training programme for that person. The individual carrying out day-to-day records management for an authority might not work for that authority directly. It is possible that the records management function is undertaken by a separate legal entity set up to provide functions on behalf of the authority, for example an arm's length body or a contractor. Under these circumstances the authority must satisfy itself that the supplier supports and continues to provide a robust records management service to the authority. The authority's RMP must confirm that it is satisfied by the standard of the records management provided by the supplier and name the organisation that has been appointed to carry out records management on the authority's behalf. Where an authority's records management system has been put in place by a third party, but is operated on a day-to-day basis by a member of staff in the authority, it is the competencies of that member of staff which should be confirmed, not those of the third party supplier of the system. Read further explanation and guidance about element 12 - http://www.nas.gov.uk/recordKeeping/PRSA/guidanceElement12.asp
Statement of Compliance	The competency framework for the post of Head of Information Governance indicates that the role holder should have or be working towards a degree or post graduate level qualification in information / records management or be working towards such a qualification. The Head of Information Governance is also a member of the Information and Records Management Society (IRMS). As part of the Records Management project, HES will be appointing IAO's and IAA's throughout the organisation and training them appropriately.
Evidence of Compliance	Evidence to be submitted in support of Element 12 includes:
	Completed and Approved Head of Records Management Person Specification Head of Records Management Job Advertisement Staff Training Logs Blank Skills Matrix IG Team Job Descriptions

	Records Management Competency Framework Corporate Membership of IRMS Head of Information Governance member of IRMS IRMS Certificate in Information Governance awarded to Records Manager MSc. Records Management and Informaton Rights enrolment for Records Manager Practitioner Cerficate in Data Protection awarded to the Information Manager
Future Developments	The Head of Information Governance will ensure that records management remains on the agenda at divisional team meetings. The current Records Management Team (now Information Governance) have been engaging pro-actively and raising awareness of the importance of records management with business areas since its inception in 2014. The team will continue to do so going forward as they are developing a dedicated training programme for all staff. The training programme will raise awareness of the importance of records management and highlight roles and responsibilities. Training will cover compliance (including Data Protection, Freedom of Information and the Public Records (Scotland) Act 2011), information security and assurance, records management processes and procedures, and sources of guidance in HES. Practical workshops on managing and accessing information will be run throughout the organisation. HES will appoint IAO's / IAA's throughout the organisation and will train them appropriately. Senior management are committed to maintaining effective records management and will ensure ongoing adequate resources are available to fulfil the requirements under the PRSA and other information legislations.
Assessment and Review	This element will be regularly reviewed throughout 2017/18 alongside the development and delivery of records management training to all staff.
Responsible Officer(s)	David Paris, Head of Information Governance

ELEMENT 13: REVIEW AND ASSESSMENT

Regular self-assessment and review of records management systems will give an authority a clear statement of the extent that its records management practices conform to the Records Management Plan as submitted and agreed by the Keeper.

Introduction	Section 1(5) (i)(a) of the Act says that an authority must keep its RMP under review.
	An authority's RMP must describe the procedures in place to regularly review it in the future.
	It is important that an authority's RMP is regularly reviewed to ensure that it remains fit for purpose. It is therefore vital that a mechanism exists for this to happen automatically as part of an authority's internal records management processes.
	A statement to support the authority's commitment to keep its RMP under review must appear in the RMP detailing how it will accomplish this task.
	Read further explanation and guidance about element 13 – http://www.nas.gov.uk/recordKeeping/PRSA/guidanceElement13.asp
Statement of Compliance	Each of the policies and procedures produced in line with the requirements of the Public Records (Scotland) Act 2011 have been done so in consultation with colleagues across the organisation. Each new policy has been reviewed in detail in order to ensure compliance with all business as well as legal obligations.
	The assessment and review of Information Governance within HES will be completed on a regular basis. This will be measured by the HMG Information Assurance Maturity Model, HES feels that this is a wider ranging model and encompasses more in the scope of Information Governance, as a concept, than focussing soley on PRSA. Although the IAMM is no longer supported as a function by the National Cyber Security Centre the IAMM has been adapted for HES to ensure it meets the needs of the organisation. The IAMM has been updated bi-annually, the results from the update are fed back into the Informaiton Governance improvement plans for the next 6 months.
	HES has employed a Head of Internal Audit and Business Improvement. The Head of Information Governance has had early discussions and agreed the entirety of Information Governance arrangements (Records Management, Data Protection under GDPR, Freedom of Information, Information Security and Information Management) within HES will be audited over the coming years in a rolling programme of audits.
Evidence of Compliance	Evidence to be submitted in support of Element 13 includes:
	Completed and Approved Records Management Strategy Information Management Strategy Information Assurance Maturity Model Information Assurance Board ToR

Future Developments	The Head of Information Governance will ensure that a second assessment review is carried out within 6/9 months following submission of the records management plan and thereafter annually. A report will be submitted to the HES Board annually on the anniversary of the approval of the RMP and once approved will be submitted to the Keeper as evidence of HES' commitment to improving record keeping in the organisation. The Head of Information Governance will continue to ensure that records management remains on the agenda at divisional meetings and the IG Team will attend these to discuss and update on records management. Once the Information Assurance Board and the IAOs are appointed the main focus will be to review and challenge the IAMM. This will ensure Information Assurance is taken seriously across the organisation and will provide focus to the work of the IG Team.
Assessment and Review	The concept of records management is new to HES and it would be prudent to give all the policies and procedures time to bed-in. All policies and procedures will be reviewed periodically during 2017/18 to ensure they remain accurate and up to date.
Responsible Officer(s)	David Paris, Head of Information Governance

ELEMENT 14: SHARED INFORMATION

Under certain conditions, information given in confidence may be shared. Most commonly this relates to personal information, but it can also happen with confidential corporate records.

Introduction	The Keeper will expect an authority's RMP to reflect its procedures for sharing information. Authorities who share, or are planning to share, information must provide evidence that they have considered the implications of information sharing on good records management. Information sharing protocols act as high level statements of principles on sharing and associated issues, and provide general guidance to staff on sharing information or disclosing it to another party. It may therefore be necessary for an authority's RMP to include reference to information sharing protocols that govern how the authority will exchange information with others and make provision for appropriate governance procedures. Specifically the Keeper will expect assurances that an authority's information sharing procedures are clear about the purpose of record sharing which will normally be based on professional obligations. The Keeper will also expect to see a statement regarding the security of transfer of information, or records, between authorities whatever the format. Issues critical to the good governance of shared information should be clearly set out among parties at the earliest practical stage of the information sharing process. This governance should address accuracy, retention and ownership. The data sharing element of an authority's RMP should explain review procedures, particularly as a response to new legislation. Read further explanation and guidance about element 14 - http://www.nas.gov.uk/recordKeeping/PRSA/guidanceElement14.asp
Statement of Compliance	This is an area that requires further development. Historic Environment Scotland operates in accordance with the Information Commissioner's Data Sharing Code of Practice. Historic Environment Scotland identify all instances of information sharing between service areas and where information is shared with or processed by a third party. This is governed by Historic Environment Scotland's agreements with third parties Data Processing Agreements (for Personal Data) and Memorandums of Understanding, Management Agreements or contracts (for Corporate Information). We have a statutory duty to respond to requests for information made under the Freedom of Information (Scotland) Act 2002 and the Environmental Information (Scotland) Regulations 2004. As part of our compliance with these statutory obligations we share information openly through our publication scheme. HES also shares data under the INSPIRE (Scotland) Amendment Regulations 2012 in which we make available, in a consistent format, spatial datasets which come within the scope of the Directive. We also share, via the Historic Environment Portal decisions and designation records. Further information on this is available via: http://portal.historicenvironment.scot/ The development of the IAR will help assist in identifying who within HES shares data and/or information and what controls there are surrounding this.

Evidence of Compliance	Evidence to be submitted in support of Element 14 includes:
	Completed and Approved Publication Scheme Guide (on website) Data Processing Agreement Gap Analysis INSPIRE (GIS) INSPIRE Spatial Data Audit 2014
Future Developments	HES will look to define specific arrangements for information sharing, including the establishment of clear information sharing protocols, dependant on the type of information being shared.
Assessment and Review	Element 14 will be reviewed in the autumn of 2017 and again in spring 2018 as new Information Sharing protocols are developed for the organisation.
Responsible Officer(s)	David Paris, Head of Information Governance.

ELEMENT 15: FREEDOM OF INFORMATION
THIS IS NOT AN ELEMENT OF THE KEEPER'S MODEL RECORDS MANAGEMENT PLAN.

Introduction	This is not an element of the Keeper's Model Records Management Plan, however HES feels that freedom of information legislation is an important part of overall information management. Under section 60 of FOISA and regulation 18 of the EIRs, Scottish Ministers may publish a Code of Practice which describes the practice which they consider would be desirable for Scottish public authorities to follow in connection with the discharge of their functions under FOISA and the EIRs. The Code provides guidance to Scottish public authorities on the practice which Scottish Ministers consider desirable for authorities to follow in connection with the discharge of their functions under the regimes. In particular it includes guidance on:- − responsibility for FOI within an authority; − handling a request for information; − training and staffing arrangements; − records management and searching for information; − the provision of advice and assistance by authorities to people who propose to make, or have made, requests for information; − responding to requests; − transferring requests to other authorities; − consulting third parties to whom information requested relates, or people whose interests are likely to be affected by the disclosure of such information; − the disclosure of contractual and procurement-related information; − responding to reviews; − monitoring compliance, collecting and recording statistics about request handling; − proactively publishing information; and − appeals to the Commissioner
Statement of Compliance	HES is committed to the discharge of its functions under FOISA and EIRs. HES has a network of FOI Lead Officers who actively respond to all requests and are proficient in the handling of those requests. HES has a Publication Scheme which is promoted on the HES Website.
Evidence of Compliance	Evidence to be submitted in support of Element 15 includes:
	Completed and Approved Publication Scheme Guide (on website) Data Protection and Freedom of Information Officer Job Description FoI Policy FoI Guidance to HES Board FoI / DPA Combined Action Plan
Future Developments	The Information Manager is designing an on-line training course covering FoI and EIR regulations which will be launched around May 2017. The Information Manager will write bespoke guidance on FoI and EIR usage and exemptions. This will be published in 2017. The Intranet will be updated as required

Assessment and Review	This element will be regularly reviewed throughout 2017/18 to ensure compliance with the regulations.
Responsible Officer(s)	David Paris, Head of Information Governance. Roger Green, Information Manager

Future Developments / Going Forward

Information Assurance Maturity Model (IAMM)

Current Position - HES needs to ensure that effective Information Risk Management processes and procedures are in place to provide assurance to the CE and SIRO that information is adequate secured within HES and that information passed to external parties is protected appropriately. To support this, HES has aligned itself with HMG's Information Assurance Maturity Model. Benchmarking HES against the 5 levels has taken place and the model itself has been amended to meet the needs of HES.

Future Developments – The IAMM will be reviewed and updated, officially, bi-annually. The results of the review process will be presented to the Information Assurance Board and actions will be fed back into the overall Information Governance Improvement plan.

Electronic Records

Current Position – HES suffers from a continued growth of largely unmanaged, unstructured electronic document and record storage – shared drives. These present a number of associated problems not least the potential breaches of statutory and regulatory requirements, lack of visibility of information, the inevitable duplication of documents and records which in turn leads HES being unable to demonstrate the key attributes of a record (authenticity, reliability and integrity). Further to this, the technical infrastructure in place does not provide the necessary functionality to allow for the effective management of the records created by HES eg retention and disposal, access and security and audit trail. In some parts of the organisation, there is a practice of printing official information to be filed on an officially registered file. In other areas, official information is also printed but it is not filed on officially registered files. In both cases, this adds not only costs to the organisation but adds the risk that not all official information is printed and filed.

It is the aim of HES to introduce an eDRMS but discussions are at an early stage. Approval in principle has been given for an eDRMS but there is much work to be done prior to scoping out such a system. There is the issue of bringing all the shared network drives across the organisation together, the migration of the records and information held in John Sinclair House into the HES Corporate Network, the cleaning up of all the data to get rid of duplicates etc and the building of the agreed file plans for each of the business areas. Some preparatory work will be undertaken during 2017/18 to understand the business requirements. The project to migrate the data to the HES network will begin in the summer of 2017.

Future Developments – The contract with RecordPoint has been signed and we are moving towards implementation over the first quarter of 2018/19. The business case to fully develop SharePoint has commenced and this will continue through the various approval stages. The approved business case will be submitted as further evidence in the annual return to NRS.

Physical Records Management

Current Position – HES's Registry Team is currently available to the former Historic Scotland branches only. The three members of the Registry Team keeps records of c125,000 files that are open, closed, destroyed or transferred to NRS for archiving.

There are a number of problems in terms of managing this service not least the space that looking after such a quantity of files poses. There is also the issue of files being transferred to users within the organisation and the Registry Team are not notified of the file movement. There is currently a project underway to reconcile what physical records the organisation holds against what is held on the registry system (IMPReS). Where there is no record of the physical file(s) on the registry system these will be added.

HES has been working to consolidate its physical records and has been working with Business Areas to close Third Party storage facilities. There are 2 facilities remaining and these will be closed in the coming months.

Future Developments – the file reconciliation project was completed in March 2017. The results of this gave an understanding of what we hold physically. The IMPReS system was also updated with any 'missing' files. The RecordPoint contract includes the ability to manage physical files more efficiently and effectively. There will be a project to migrate the management of the physical files from IMPReS to RecordPoint. There is also now an opportunity to look at and re-evaluate the physical records management needs across HES. There has been no registry provision for the former RCAHMS staff and there is now an opportunity work with those business areas to see if there is a need for a registry function

Information Governance Training

Current Position – the Head of Information has qualified with MSc. (Merit) in Records Management and Digital Preservation. The Information Manager undertook study during 2016/17 and obtained a Practitioner Certificate in Data Protection. The Records Manager has also obtained the IRMS Foundation Certificate in Information Governance and is now enrolled in MSc. Records Management and Information Rights with University of Dundee. The general level of recordkeeping awareness within HES is improving following the recent information audits and the work the Information Governance Team undertook designing file plans and retention schedules. However, it could be much better and there is an opportunity to build on the recent work by increasing team visibility across the organisation.

Future Developments – HES will look to produce and deliver comprehensive information governance training to all staff in order to raise the awareness of the importance of records management as well as highlighting roles and responsibilities. The training will cover:

- Data Protection (revised for GDPR);
- Freedom of Information;
- The Public Records (Scotland) Act 2011;
- Information Security and Assurance;
- Records Management processes and procedures; and
- Sources of guidance

Records Management Training

Current Position – formal training in records management generally has not occurred in the current or predecessor organisations for some considerable time. Those business areas that use the Registry for their paper files have some knowledge but it is mainly restricted on to how to open, close and review files.

Future Developments – the Information Governance Team are currently writing a number of polices and guidance notes on topics such as version control, naming conventions, managing emails, retention and disposal and using the file structures properly. A full comprehensive training package covering these topics as well as those listed under information governance will be designed and delivered to all staff during 2017/18.

Data Protection and Freedom of Information

Current Position – The data protection policy has been revised for GDPR, approved and published on the staff intranet. Similarly, the Subject Access Request, the Privacy Impact Assessment guidance and the Surveillance Systems Code of Practice have been approved. Staff will be made aware that guidance on these subjects exists. In terms of Freedom of Information, the network of FoI leads within the departments remains with overall guidance from the Information Manager.

Future Developments – the Information Manager is designing an on-line training course covering FoI and EIR regulations which will be launched around Autumn 2018. This will complement the on-line training already available on DPA and Information Security. The Information Manager will write bespoke guidance on FoI and EIR usage and exemptions. This will be published in 2017. Bespoke DPA training for regional offices has been piloted and will be rolled out to the other regional offices during 2017. The Intranet will be updated as required.