HES ARCHIVES:

DIGITAL REPOSITORY MANAGEMENT POLICIES

HISTORIC ENVIRONMENT SCOTLAND | ÀRAINNEACHD EACHDRAIDHEIL ALBA

1. INTRODUCTION

HES has been actively developing a Digital Repository to ensure the long-term preservation of contemporary records which illustrate or document the historic environment of Scotland.

This is essential for the survival of unique digital records and for the continuing development and currency of the HES Archive. Digital records contribute to telling Scotland's story but will also provide sources of information for future generations.

This suite of documents sets out the purpose, guiding principles and operational policies for the Digital Repository.

2. DOCUMENT CONTROL

HES Archives: Digital Repository management policies are published on the HES website and will be reviewed every three years. The next review date for this policy will be no later than October 2022.

Relevant parties will be notified of any changes to this policy and the implications of any changes for the future of existing digital collections.

For further questions about the HES Archives: Digital Repository management policies please contact Digital.Archives@HES.scot

Cover image: Orthoimage of laser scan data at Castle Dounie.
canmore.org.uk/collection/1568680

3. DEFINITIONS

HES Archives

The functions of HES are set out in the *Historic Environment Scotland Act 2014* (i) and include management of its physical and digital archives as a national resource for reference, study and research.

The HES Archive comprises collections of national and international importance and is a key component of the National Record of the Historic Environment. Contents of the archive stem from survey, recording and research by HES and other individuals and organisations; from the integration of different organisations and their archives; and active collecting of archives from individuals and organisations relating to the historic environment of Scotland

Digital Repository

HES Digital Repository is an infrastructure which stores manages, publishes and curates digital assets relating to the historic environment of Scotland. This includes software and hardware technologies, policies, processes, services, and people, as well as content and metadata.

HES Digital Repository is underpinned and supported by IT staff and dedicated digital archive staff who form part of the wider HES Archives.

Digital Object

Individual digital files (that may comprise a larger digital collection)

Digital Content/Material

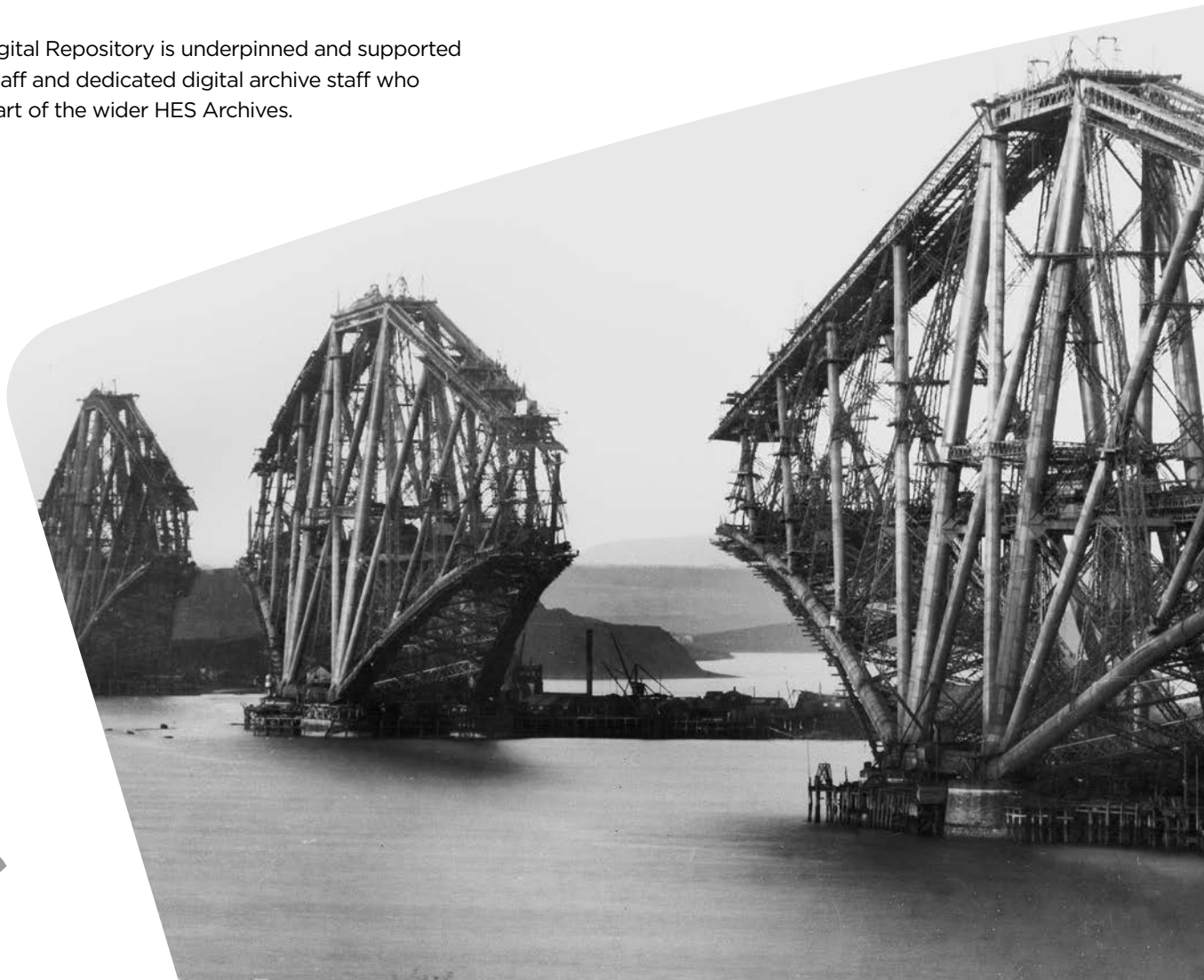
A diversity of digital material that forms part of an archival collection (may be part of archival deposits containing physical, analogue and digital objects)

Digital Collections

Curated collections of digital objects (may be associated with related physical materials)

Digital Assets

Digital objects and collections that are recognised to have a long-term value. These are collected according to their accuracy, integrity and authenticity, their provenance and their long-term durability and usability.



View of the Forth Bridge under construction. canmore.org.uk/collection/370937

4. MISSION STATEMENT

HES Archives are managed in accordance with the functions as set out in the *Historic Environment Scotland Act 2014* (i), *UK Public Records Acts 1958* (ii) & *1967* (iii), and the *Public Records (Scotland) Act 2011* (iv).

With increased volumes of digital material HES has established a digital repository. This is aligned with the wider HES organisational community and strategies in relation to stewardship and management of digital materials and the curation of an open and accessible archive that is preserved for use by future generations.

Our mission is to:

- manage our cultural heritage digital collections across the entire digital curation lifecycle according to international standards and domain best practice
- ensure wide and continued access to our internationally significant digital collections for future generations
- support and anticipate the evolving digital needs of users interested in local and family history, architecture, archaeology, as well as the industrial and maritime environment
- collaborate and innovate to enhance knowledge and understanding of Scotland's historic environment

HES Archives aims to serve a broad community, encompassing local, national and international audiences. This community comprises both users and stakeholders from the general public and from those with more defined professional and research agenda including:

- commercial archaeological units
- architectural practices
- engineering companies
- developers and related firms
- university and college researchers, students and staff
- independent researchers, both local and international
- HES staff
- staff from related heritage bodies
- members of Scottish Government
- the police, fire services and armed forces
- schools
- community heritage organisations
- broadcast and other media
- charities
- the creative industries

5. COLLECTION POLICY

5.1 Policy statement

We are committed to acquiring and preserving digital assets that contribute to a public record of Scotland's historic environment and to delivering high-quality and curated digital collections for use by all in our designated community as stated in the *HES Archives: Digital Repository Mission Statement* (see 4.), both now and for future generations.

This policy complements and is informed by the *HES Archives and Collections Development Policy, 2017-2020* (v) and applies to one area of collecting, namely the National Record of the Historic Environment.

The policy sets out the purpose and guiding principles adopted by HES for the acquisition and disposal of digital material. It resonates with the digital archive's mission to support and anticipate the evolving digital needs of users interested in local and family history, architecture, archaeology, as well as the industrial and maritime environment.

5.2 Scope

New acquisitions of digital materials are made according to the following collecting criteria:

- Digital material relating to the historic environment of Scotland, including architecture, archaeology, industry and maritime
- Digital material created during survey, recording and research activities across HES

We acquire or accept digital materials principally for Scotland and its regions though not exclusively so. In most cases assets held in the digital archive are unique copies and cannot be found elsewhere.

HES Archives makes efforts to confirm that all digital materials are collected in accordance with legal and ethical criteria in place at the time. Where this information is unavailable, the professional judgement of senior archive managers will be used to decide on the inclusion of such material taking into account any relative risk associated with it.

5.3 Acquisition

We evaluate and acquire digital materials offered based on our collecting criteria, their intellectual content and potential re-use, and relative digital preservation requirements (e.g. costs, completeness, media, technical documentation). We may consider digital objects that do not meet all these criteria, particularly if there is significant re-use value or historical significance. Instead, documentation accompanying such digital materials may be amended to highlight any re-usability issue.

We offer depositors a list of preferred and accepted formats that HES Archives considers best suited for long-time preservation and continuity of access. The formats are commonly used within the archaeology and architecture domains, have open specifications, and are independent of specific software, developers or supplier. These include formats for digital images, documents and raw text as well as more complex digital objects (vi).

Digital material such as vector graphics (e.g. CAD drawings), geophysical and topographic survey data, relational databases and spatial data often necessitate additional digital preservation actions in order to maintain their future functionality. These include contingent digital file requirements, complexity and variety of data formats and structures, proprietary formats, the need to maintain the technical and social contexts in which the data exists, as well as growing importance of web services, new technologies and advanced delivery and analytical environments.

Where questions arise about the suitability of a dataset for the archive or its re-use potential is unclear, we will seek advice from domain practitioners within HES to assist with the evaluation process and maintain the high standards necessary for the effective development of a quality national archive.

5.4 Metadata and documentation

We require depositors to provide appropriate metadata and documentation to enable us to both preserve and make digital files accessible.

To promote resource discovery we need Site and Project-level metadata, as well as File level metadata and Technical metadata for more complex digital objects.

Where practicable we also require that digital objects are accompanied by comprehensive machine-readable contextual documentation including file inventories, technical notes, reports, and errata in open and accessible formats. Non-digital documentation may be digitised if required.

In cases where metadata or documentation is insufficient, we will work with depositors to ensure that digital files are useable and understandable by generating additional contextual information.

5.5 Appraisal

Appraisal is the process of selectively retaining or disposing of digital objects in a transparent and accountable way. This activity is critical for identifying areas for future collection development, either by considered rationalisation or through retention scheduling. Although there is a presumption against disposal, we recognise that responsible, curatorial motivated disposal is one of the tools that can be used for developing collections.

We appraise digital objects according to the following principles:

- digital objects meet the criteria of the archive as set out in 5.2 (above)
- digital objects are unique and are not duplicates of, or similar to, other objects in the collections
- digital objects meet the standards and accepted formats in 5.3 (above)
- digital objects deemed to be inadequately documented; are potentially disclosive; are acquired or generated illegally; or are suspected or known to contain inaccuracies.

We operate with internal and external appraisal guidance for digital archive staff and depositors respectively.

5.6 Disposal

We are committed to ensuring that digital material we hold in the repository is preserved and made available for people to use. However, we are also committed to ensuring that material is archived and displayed lawfully and appropriately.

There is a strong presumption against the disposal of any objects in the digital repository except in exceptional circumstances. These include:

- A record contains personal or sensitive personal information about a living individual and continued access to this would be unlawful or unfair under the General Data Protection Regulation (GDPR) (vii), Data Protection Act 2018 (viii) or the Human Rights Act 1998 (ix).
- A digital object is not unique and is a duplicate
- A digital object is no longer of use for the collection due to deterioration, corruption or damage e.g. through obsolescence, bit rot
- Information or images were obtained illegally

We will ensure that the disposal process is carried out openly and with transparency through the established formal review process. Full records will be kept of all decisions on disposal and the items involved and proper arrangements made for the preservation and/or transfer, of the documentation relating to the items concerned. This includes digital images where practicable in accordance with recognised professional standards on deaccession and disposal.

We will restrict access to digital objects that may be subject to a copyright enquiry or an ‘embargo’ publication period with metadata record only remaining in the public domain.

6. SUBMISSION POLICY

6.1 Policy statement

We are committed to acquiring and preserving digital assets that contribute to a public record of Scotland's historic environment and to delivering high-quality and curated digital collections for use by all in our designated community as stated in the *Mission Statement* (see 4.), both now and for future generations.

This policy sets out the preconditions by which digital objects will be submitted and accepted into the HES Archives.

6.2 Scope

We accept transfers of digital objects from depositors through set channels such as on physical storage media and secure file transfer. We will work closely with depositors to ensure that all digital objects comply with preferred and accepted formats and are accompanied by appropriate discovery metadata and contextual documentation.

Digital objects submitted will be published only when they have been quarantined, appraised, accessioned, and catalogued against minimum standards and verified by Digital Archive staff.

6.3 Depositors

Deposits come from a variety of sources as indicated in the *Mission Statement* (see 4.). Subjects covered include Scottish history, architecture, archaeology, as well as the industrial and maritime environment. HES also transfers internally the products of its own research, survey and recordings programme to the archive for long-term preservation and public access.

6.4 Assets

Digital assets include anything that has been created in a digital format i.e. is 'born' digital or is a digital surrogate of a physical object. This can include digital photographs, survey reports, raw laser survey or geophysical data, GIS data, CAD drawings, 3D scans or illustrations.

Digital objects submitted for deposit are processed in tandem with the physical archive. Depositors are requested to make it clear, through folder structuring, file naming conventions, and inventories, any collection relationships which may already be in existence. Digital objects which do not directly adhere directly to the *HES Archives: Digital Repository Collections Policy* (see 5.) are not to be included in the deposit, for instance, HES Archives will not retain images of vehicles, animals or people unless they are clearly relevant.

Oblique aerial view centred on the remains of Castle Law fort and excavation trenches. canmore.org.uk/collection/1138819

6.5 Volume

There is no current restriction on file size or volume (though delivery of digital assets by secure file transfer may have network bandwidth or imposed transfer limits e.g. for Dropbox each folder must be less than 20 GB in total size and/or contain fewer than 10,000 files total).

We follow set appraisal procedures as detailed in the *Collections Policy* (see 5.) in order to organise and rationalise deposits for ingest into the archive. In cases of large volume deposits we will use judgement to re-arrange and structure according to the catalogue hierarchy.

6.6 Copyright

In order to accept digital material into the repository and to ensure long-term preservation, we require that depositors accept the *HES Archives Deposit Agreement* (x) summarised below:

- physical ownership of archive material must be transferred to HES via a signed Deposit Agreement to aid its successful curation.
- Intellectual Property Rights (including Copyright) of the archive must be established, and any special conditions attached to material made clear at the time of deposition with HES.
- Intellectual Property Rights can be transferred to HES as part of the Deposit Agreement. If a depositor wishes to retain Intellectual Property Rights for the material they have created then a licence must be signed to allow HES to disseminate material as per their advertised terms and conditions.
- Depositors must provide licenses for third party material allowing its dissemination by HES
- In the event of an organisation holding copyright ceasing to exist, notification of this should be made to HES, as soon as possible, with details of any new arrangements.

We will deploy open licensing frameworks where applicable and or necessary, to comply with research funding requirements and service obligations including Creative Commons and Open Government Licences with the terms of use of digital assets and any attribution included. HES also utilise a range of open mapping products for the purposes of site identification, context navigation, resource location, and spatial data download.

6.7 Withdrawal

Digital objects, assets or collections (see Definitions) can be placed under embargo for a specified period where appropriate.

In cases of removal of digital objects from the public catalogue metadata records will remain visible with a note of the withdrawn record, but the digital contents will not be viewable or downloadable.

6.8 Standard requirements

We are responsible for complying with government and industry requirements to make sure all digital collections relating to the historic environment are accessible and maintained for future use. Data standards underpin the information we curate and publish. They ensure that our digital objects are recorded consistently, are discoverable and easily searchable.

A catalogue record must be created for each digital object deposited. We ensure that each record is valid in accordance with the requirements of a set of Minimum Record Standards.

To be accepted into HES Archives and published, digital assets must conform to the following requirements:

- All texts and supporting images that may comprise a final report or publication should form the core of the digital deposit.
- Any supporting graphics that are embedded into a final report but which are also available in higher resolution or uncropped should be included as separate items.
- All raw (unprocessed) data relating to various specialist activities should be included where possible. If unprocessed data is not available in digital form, and provision cannot be made to scan it electronically, it can be supplied to HES as hardcopy. Adobe Portable Document Format files are accepted. However, any constituents that go to make up the PDF file (e.g. TIFF files, Microsoft Word document) should be documented and supplied as well.
- Depositors should not provide digital objects in more than one file format if their content is identical, unless the original format is known to be at risk. When submitting digital images depositors should avoid duplicate, near duplicate or extraneous images. Where a document exists in several versions, only supply the final (non-draft) version

with the assemblage. Written correspondence (electronic or scanned hardcopy) relating to the project should not be included unless it represents a primary aspect of the project's brief or adds value to the assemblage. No material should be included that may be interpreted as being defamatory or libellous to any living person.

We also need contextual documentation for the deposited archive. This includes:

Technical documentation: information about items, or groups of items, within the archive which will enable the data to be understood and reused by others. This also encompasses documentation relating to third party material that may be embedded within the resource being deposited. Technical documentation should be submitted with the archive in electronic form only.

Formats and conventions: Wherever possible, depositors should supply digital material in preferred or accepted standards as detailed in the *Guidelines for Archiving of Archaeological Projects Appendix C* (vi) This includes a list of recommended file formats for a range of data types relating to archaeological and architectural activities. Bespoke text file formats developed by depositors for very specific and specialised purposes are acceptable, provided that adequate information is supplied concerning the files' internal data structures.

Where the original format used is bespoke, very newly developed and/ or not widely accepted depositors may supply a single item in more than one format.

6.9 Validation and approval

All submissions will be validated against minimum requirements and collecting criteria by staff. If the submission is deemed out of scope of the *Collection Policy* (see 5.) it may be rejected.

If the submission is in scope of the *Collection Policy* (see 5.) but fails to meet the minimum requirements it will be returned to the Depositor with a request for the required information/data.

We may modify metadata elements to correct minor errors, ensure consistency with our policies, and add administrative metadata, but will not make substantive modifications to descriptive metadata without the prior approval of the Depositor. We will not check the accuracy and authority of the content of submissions. These are the sole responsibility of the Depositor.

Once a submission has been ingested, catalogued and approved it will form part of HES Archives.

7. PRESERVATION & STORAGE POLICY

7.1 Policy statement

HES Archives are an integral part of Historic Environment Scotland (HES). We are committed to safeguarding and protecting the cultural significance and integrity of our digital collections for the benefit of the public.

This policy sets out the purpose and guiding principles adopted HES for the long-term storage and preservation of digital objects in its collections. It relates closely to and is informed by the *Collections Policy* (see 5.) and *HES Archives and Collections Development Policy* (v).

7.2 Scope

This policy applies to all digital objects in the control and management of HES Archives and aligns with the Digital Repository mission to:

- manage our cultural heritage digital assets across the entire digital curation lifecycle according to international standards and domain best practice
- ensure wide and continued access to our internationally significant digital collections

The *Preservation & Storage Policy* is informed by a variety of community-driven standards. These include the *Open Archival Information Systems (OAIS) reference model* (xi), *Trusted Repositories Audit and Certification (TRAC)* (xii), *Core Trust Seal* (xiii), *National Digital Stewardship Alliance (NDSA)* (xiv) and represent an international body of knowledge and expertise relating to various issues within digital preservation.

7.3 Digital preservation

We are committed to ensuring that all digital assets held are preserved and made available for people to use. However, we are also committed to ensuring that material is archived and displayed lawfully and appropriately.

In line with the *Collections Policy* (see 5.) we follow a set of detailed internal processes and guidelines to ensure the authenticity, integrity and provenance of HES digital assets.

Upon receipt of new digital content, we work with depositors to ensure digital objects are accompanied with metadata and supporting technical or contextual documentation, to resolve irregularities with digital objects, and migrate file formats if necessary. We will also address ethical, privacy or rights management so that digital deposits can be fully understood and re-used in perpetuity.

Depositors are offered a list of preferred and accepted file formats that we considers best suited for long-time preservation and continuity of access. The file formats are commonly used within the archaeological and architectural domains, have open specifications, and where possible independent of specific software vendor. Non-standard formats will be considered for ingestion where necessary, such as in the case of rescue-type deposits.

All newly acquired digital objects go through a quarantine process and are check-summed prior to transfer into a non-public Accessions database. Checksums are also created upon ingest from the Accessions database and stored within a table of an Oracle Application Express (Apex) database. (A backup of the Apex database is taken every night and is retained for a finite period according to current best practice). To ensure data integrity an automated fixity script is run every night to validate each object against the stored checksum to verify checksum, permissions, and record counts.

The original bitstream of all digital objects is retained once objects have been ingested and catalogued into the Oracle Application Express (Apex) database and form part of the national record. Requests for withdrawals, revisions or deletions are monitored and

Wooden carved cherub in situ at the wreck off Duart Point. canmore.org.uk/collection/1127028

logged through a formal audit and review process as outlined in the *HES Archives: Digital Repository Collections Policy* (see 5.6) and internal guidance for managing rescans of digital images.

Digital Archive staff can withdraw or restrict access to digital objects, as outlined in the *HES Archives: Digital Repository Submission Policy* (see 6.7). Acceptable reasons for withdrawal include copyright violation, data protection infringement, material considered defamatory, obscene or contravene equalities or diversity legislation, or digital objects published online in error. For withdrawn items the original metadata record is marked as superseded with a note detailing the replacement object. The permanent link to metadata record remains in the public domain to avoid broken links. Under specified circumstances, conditions and following agreed procedures digital objects can be deleted by staff.

In the event of a major incident, HES has in place appropriate business continuity plans for the Digital Repository.

By way of succession planning the Digital Repository will work in accordance with existing agreements and procedures to fully transfer digital assets and contextual documents to the National Records of Scotland to ensure the preservation of material beyond the existence of the Digital Repository.

7.4 Storage

We accept transfers of data from depositors through set channels on physical storage media and secure file transfer. Original storage media is retained within archival quality storage folders which prevents oxidisation and neutralised corrosive gasses to prevent fungus and bacterial growth. These are then stored within our climate controlled archival strong rooms which are managed and controlled by professional preventative conservators.

The Digital Repository is presented as a network share hosted by a virtual server running Microsoft Server operating system and using storage from an enterprise class Storage Area Network. The Digital Repository share is automatically replicated to a backup container offsite at DataVita as well as in Amazon Glacier/Cloud.

The Digital Repository primary contents are backed up daily to disk. A backup policy creates a full copy of the primary archive every 30 days and is retained for 90 days and 3 copies. For additional resilience, an "auxiliary" copy of the archive data is made to tape and moved off-site to a secure location. The same retention policy applies to tape.

7.5 Security

The Digital Repository technical infrastructure is protected by HES IT & cyber security protocol and policies (xv) developed and maintained by outsource partner Protocol Policy Systems Ltd. The policies provide a security and acceptable-use framework for Historic Environment Scotland as an organisation. These are published on the HES intranet to safeguard HES security systems and for HES staff.

The digital repository is secured by a hardware Firewall. All digital information is stored in a database behind this to ensure confidentiality. The database system is password protected and only staff with special permissions may access the system.

7.6 Preservation watch

Preservation activities within the Digital Repository require research and updating to keep pace with changing technologies. To guarantee that preservation activities remain valid, we have an ongoing programme of research and review of preservation options, updating and refining processes as required. To meet this aim, we:

- Collaborate with the international community to monitor contemporary and emerging standards, formats and hardware, software and storage technologies.
- Consider user community definitions, and their associated competences and knowledge base, when developing preservation activities to ensure digital objects remain suitable for their needs.
- Develop, implement and review preservation strategies for the types of objects we hold in the Digital Repository, including specifications for metadata to be captured during preservation activities to ensure they can be accessed in perpetuity
- Conduct periodic staff skill audits to ensure expertise and capability is developed.

8. OPERATIONAL POLICY

8.1 Policy statement

This policy sets out the guiding principles adopted by Historic Environment Scotland (HES) for the long-term care and accessibility of digital objects in its Digital Repository.

This is not a technical document and does not describe implementation nor infrastructure in any detail.

HES Archives are accessible in person in the HES Archive search room and via https://canmore.org.uk/, an online catalogue of Scotland's archaeology, buildings, industrial and maritime history. The Digital Repository is designed to be scalable and highly resilient.

8.2 Functionality

The Digital Repository includes a quarantine facility, an accessions database, an Oracle Application Express (Apex) database and file server, data centre(s) storing and hosting data, metadata schemas based on international standards, search and browse facilities, item-level usage statistics, time-stamped submissions and permanent identifiers. HES Archives are accessible via https://canmore.org.uk/, a web-based system which manages, publishes, licenses and shares digital assets for discovery and re-use.

Depositors include:

- architectural practices
- commercial archaeological units
- engineering companies
- developers and related firms
- university and college research students and staff
- independent researchers
- HES staff
- staff from related heritage bodies

HES Archives operates according to a set of policies. These include a mission statement, collections policy, submission policy, preservation and storage policy, operational policy, privacy policy, security policy, terms and conditions, depositor agreements.

8.3 Availability

Target availability for online access is 99.5% measured over a year, excluding planned maintenance periods. Core hours of support are 9AM to 5PM during working days.

There is no regular scheduled maintenance period, with all routine maintenance able to be performed without service loss. Any reduction in performance or resilience during maintenance periods will be managed to reduce affect.

8.4 Usage

Access to HES Archives via https://canmore.org.uk/ is provided solely through Terms and Conditions and User Licence. Use of this website automatically indicates an agreement to those Terms & Conditions and User Licence and are contractually binding.

HES Archives are open and available via https://canmore.org.uk/ for personal, individual and educational use. The permissions are detailed in the User Licence. Where copyright is not owned by HES or the Crown some limitations on use exist to reflect intellectual property rights.

8.5 User Risk

HES Archives make every effort to ensure all digital materials are legally uploaded. Prompt action will be taken to remove material that violate copyright, infringe data protection, are considered defamatory, obscene or contravene equalities or diversity legislation, or have been published online in error. This process will be carried out openly and with transparency through a formal audit and review process.

8.6 Resilience & replication

The service is designed to be highly resilient. The Digital Repository is presented as a network share hosted by a virtual server running Microsoft Server operating system and using storage from an enterprise class Storage Area Network. The Digital Repository share is automatically replicated to a backup container sited offsite at DataVita as well as in Amazon Glacier/Cloud.

8.7 Backup & retention

HES Digital Repository primary contents will be backed up daily to disk. A backup policy creates a full copy of the primary archive every 30 days and is retained for 90 days and 3 copies. For additional resilience, an "auxiliary" copy of the archive data is made to tape and moved off-site to a secure location. The same retention policy applies to tape.

8.8 Disaster Recovery

The primary solution in the event of a major failure at either physical site is to continue service at the remaining site. In the event of data corruption affecting both sites (data corruption or deletion being automatically replicated) or a major external event, a service copy can be restored from Amazon Cloud (or tape backups).

8.9 Planning

HES Archives will develop and maintain business and operational plans to mitigate against risks such as funding and resourcing adjustments, changing technologies and domain practices that may impact the successful curation of digital objects.

As such HES will:

- recognise and support the routine management and maintenance of the Digital Repository as a core function of the organisation
- encourage and support emerging technologies that futureproof digital archival practices
- maintain and develop a scalable and resilient IT infrastructure for the Digital Repository capable of coping with data storage and processing and the complexity of functions required
- implement systems and processes to guarantee the integrity, authenticity and security of the digital objects held within the Digital Repository.
- maintain system stability to ensure maximum uptime for services

8.10 Support

User support is provided by Digital Archive staff. Any problem reports or queries should be mailed to Digital.Archives@HES.scot. Digital Archive staff are available for consultations or extended support according to demand. Online documentation and guidance are available.

View of four surveyors outside unidentified building. canmore.org.uk/collection/1164497

9. SUMMARY OF HES IT POLICIES AND PROCEDURES

HES IT & cyber security protocol and policies have been developed and maintained by outsource partner Protocol Policy Systems Ltd and provide a security and acceptable use framework for Historic Environment Scotland as an organisation (i).

The protocols and policies address the need to protect confidential and sensitive information held on HES networks and computing equipment from disclosure, unauthorised access, loss, corruption and interference, and are relevant to information in both electronic and physical formats. They also help ensure that information is only made available or disclosed to those authorised to use it, that data integrity is safeguarded, and that information is accessible and useable on demand by those authorised to do so.

The policies are also designed to protect users, stakeholders and the organisation from illegal or damaging actions through inappropriate or unauthorised use of computer systems, communications systems and networks.

HES Information Assurance Board (IAB) are responsible for approving the strategic direction of IT to ensure that it meets the needs of the business. The IAB work closely with the Director of Corporate Services who has overall responsibility for IT within the organisation including the provision of infrastructure, applications and communications, the Head of IT who is accountable for the deployment, use and security of technology, the Information Governance Team responsible for all corporate information within HES and ensuring that effective policies and procedures are in place, and the Chief Technical Officer (CTO) who is accountable for HES's technology strategy, technology architecture and design, and architecture governance.

All users have a responsibility to ensure they are familiar with the Policies and abide by them. All policy breaches are handled in accordance with existing disciplinary procedures and may result in action up to and including dismissal.

HES IT Policies comply with a broad range of international codes, standards, regulations, frameworks and guidelines including GDPR; Computer Misuse Act 1990; Privacy and Electronic Communications (EC Directive Amendment) Regulations 2015; Intellectual Property Act 2014; Public Sector Network Cyber Essentials Plus; COBIT; ITIL; ISO9000.

HES IT Policies are also in compliance with a number of international security standards. These include:

- ISO 27002 - Organisational security management
- ISO 22313 - Resilience and business continuity management
- ISO 27017 - Cloud-based technology security controls
- ISO 29151 - Personally Identifiable Information (PII) protection-specific controls

HES IT Policies are regularly monitored and reviewed to ensure that they remain relevant to Historic Environment Scotland's business aims and objectives and in the event of the introduction of new or upgraded technology. A review of Policies may be instigated in the event of a security incident in order to prevent a similar occurrence. The Head of IT will monitor staff compliance to the Policies, associated standards and procedures on an ongoing basis. Training needs will be identified and continuous offending will be escalated to Managers and above.

10. HES SECURITY AND IT POLICY SUMMARY

This summary briefly outlines each Security and IT Policy in effect and as they apply to the Historic Environment Scotland networks, systems and equipment.

10.1 Acceptable Use Policy

The Acceptable Use Policy ensures that all computer systems and networks owned or managed by HES are operated in an effective, safe, ethical and lawful manner and it is the responsibility of every computer user to know these requirements and to comply with them.

10.2 Access Control Policy

The Access Control Policy ensures that information systems resources and electronic information assets owned or managed by HES are available to all authorised personnel. The Policy also deals with the prevention of unauthorised access through managed controls to create a secure computing environment.

10.3 Anti-Virus Policy

This Policy is about protecting networks, systems and equipment from malicious code and malware. Laptops and mobile devices are most at risk as they may only be connected to the network periodically. The appropriate use of Anti-virus software will lessen the risk of the HES experiencing this type of security incident.

10.4 Business Continuity/DR Policy

The IT Business Continuity/DR Policy ensures that HES has the appropriate resources available for planning, establishing, implementing, operating, monitoring, reviewing, maintaining and continually improving a Business Continuity/DR capability that will enable the organisations to prepare for, respond to and recover from disruptive incidents when they arise. The scale of events covered by this Policy ranges from minor or partial system unavailability (business continuity) through to total system loss (disaster recovery).

10.5 Cloud Computing Policy

The Cloud Computing Policy ensures that the confidentiality, integrity and availability of the HES's information is maintained when services are delivered through a cloud computing environment. As the cloud can be private or public, local or international it is important to ensure that arrangements are supported by a Service agreement, meet the HES's requirements for information security and enable statutory and legislative obligations to be met.

10.6 Communication and Mobile Devices Policy

The Communication and Mobile Devices Policy advises on acceptable use with regard to mobile devices (including mobile phones) and communication systems used for business activities. With the convergence of data and voice and video communication systems the ability to connect remotely to internal systems and the wide range of options offered by mobile devices it is essential that these technologies be used by authorised persons for legitimate business activities.

10.7 Computer Systems and Equipment Use Policy

The Computer Systems and Equipment Use Policy advises users of the HES's expectations regarding the acceptable use of the technology provided to them.

10.8 Computers for Board Members Policy

The Computers for Board Members ensures that computers supplied for HES business are managed, maintained and operated in accordance with HES requirements.

10.9 Cyber Crime and Security Incident Policy

The Cyber Crime and Security Incident ensures that the correct procedures are followed should systems be affected by a security incident or other event. The impact an event will have on business continuity will depend on how well it is handled.

10.10 Email Policy

The purpose of the Email Policy is to document how electronic mail systems and services are to be used. Email has become a major communication channel and a common means of conducting day to day business. Compliance with these Policies is essential to ensure that important email documents become part of the corporate knowledge-base and to ensure compliance with information management and legal requirements.

10.11 Encryption Policy

The Encryption Policy ensures that encryption keys are securely managed throughout their life cycle. This includes their creation, storage and the manner in which they are used and destroyed.

10.12 Firewall Management Policy

The Firewall Management Policy ensures that the external perimeter defence for HES is configured, managed and maintained to prevent the occurrence of a major security threat.

10.13 Hardware Management Policy

The Hardware Management Policy ensures that the correct procedures are followed with regard to the purchase, deployment, maintenance and replacement of computer hardware and other devices.

10.14 Information Management Policy

The Information Management Strategy and Policy sets out the guidelines for managing the data and information stored in the files and directories that comprise the electronic information repositories of HES.

10.15 Internet Use Policy

The Internet Use Policy ensures that the internet is used for business purposes at Historic Environment Scotland (HES) and to ensure that users conduct their online activities in an appropriate, responsible and ethical manner.

10.16 Laptop and Tablet Security Policy

The purpose of this Policy is to inform those who have been allocated a laptop computer or tablet of the HES's requirements for its use and care. Theft, loss or damage to portable computers is becoming increasingly commonplace. The costs of replacement are not just financial and include loss of data, lost productivity, increased insurance premiums and the time to configure and set up a new machine. There are also risks associated with the loss or exposure of sensitive, unique or personal information including reputation, commercial advantage and privacy and this Policy seeks to mitigate these risks.

10.17 Legal Compliance Policy

The Legal Compliance Policy ensures that staff understand the implications of privacy, confidentiality, copyright, intellectual property, misrepresentation and other relevant legislation in respect to information and information systems.

10.18 Network Management Policy

The Network Management Policy protects HES's internal computer systems and networks from abuse or exploitation and defines the parameters for managing, designing and connecting to the HES's computer systems.

10.19 Online Services Policy

The Online Services Policy provides the guidelines for configuring systems to safely enable business to be carried out over the Internet as an alternative service channel. The term "business" can apply to anything from providing information online to making payment for a service online and using online services.

10.20 Password and Authentication Policy

This Policy describes the authentication requirements for accessing internal computers and networks and includes those working in-house as well as those connecting remotely. Every person, organisation or device connecting to internal IT resources and networks must be authenticated as a valid user before gaining access to HES's computer systems, networks and information resources.

10.21 Personnel Management Policy

The Personnel Management Policy ensures that those using and managing HES's computer systems and networks act in a responsible and ethical manner. It is also intended to minimise the threat of an internal security breach.

10.22 Physical Access Policy

The Physical Access Policy protects HES's IT resources from harm, abuse or exploitation and describes the parameters for controlling the environmental conditions for critical computing devices.

10.23 Remote Access Policy

This Policy describes the security requirements for remote access connections to internal IT resources. It covers a wide variety of technologies and methods of effecting the connection.

10.24 Software Management Policy

The Software Management Policy ensures that the correct processes and procedures are followed when purchasing, developing, deploying, maintaining and replacing software applications. It assists with compliance with industry standards, encourages consistency throughout HES and ensures that software continues to meet the needs of the business.

10.25 Special Access Policy

Special Access relates to System Administrator and Domain Administrator rights. The purpose of the Special Access Policy is to ensure that only those users needing special access rights and enhanced privileges to manage the HES's computer systems and networks are granted them with the appropriate controls.

Photograph of Raasay Pictish cross slab during laser scanning. canmore.org.uk/collection/1551208

11. REFERENCED DOCUMENTS

(i) Historic Environment Scotland Act 2014 - http://www.legislation.gov.uk/asp/2014/19/contents/enacted

(ii) UK Public Records Acts 1958 - http://www.legislation.gov.uk/ukpga/Eliz2/6-7/51

(iii) UK Public Records Acts 1967 - http://www.legislation.gov.uk/ukpga/1967/44/contents

(iv) Public Records (Scotland) Act 2011 - http://www.legislation.gov.uk/asp/2011/12/contents

(v) HES Archives and Collections Development Policy, 2017-2020 - https://pub-prod-sdk.azurewebsites.net/api/file/56316fba-3068-4a14-899d-a87e009dc871

(vi) Information Guidelines for Archiving of Archaeological Projects Appendix C - https://canmore.org.uk/sites/default/files/ArchaeologyDepositorsGuidelines_2016v1_0.pdf

(vii) General Data Protection Regulation (GDPR) - https://eugdpr.org/

(viii) Data Protection Act 2018 - http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

(ix) Human Rights Act 1998 - https://www.equalityhumanrights.com/en/human-rights/human-rights-act

(x) HES Archives Deposit Agreement - https://canmore.org.uk/content/depositors-information

(xi) Open Archival Information Systems (OAIS) reference model - http://www.oais.info/

(xii) Trusted Repositories Audit and Certification (TRAC) - https://www.crl.edu/archiving-preservation/digital-archives/metrics-assessing-and-certifying/trac

(xiii) Core Trust Seal - https://www.coretrustseal.org/

(xiv) National Digital Stewardship Alliance (NDSA) - https://ndsa.org/

(xv) Historic Environment Scotland IT Policy system Implementation Case Study - https://protocolpolicy.com/historic-environment-scotland-case-study-preview/

HES ARCHIVES: DIGITAL REPOSITORY

Historic Environment Scotland is responsible for an extensive archive documenting and illustrating Scotland's archaeology, buildings, industry and maritime heritage. We are continually developing our archive collections, through both external archive deposits and internally generated survey, recording and research.

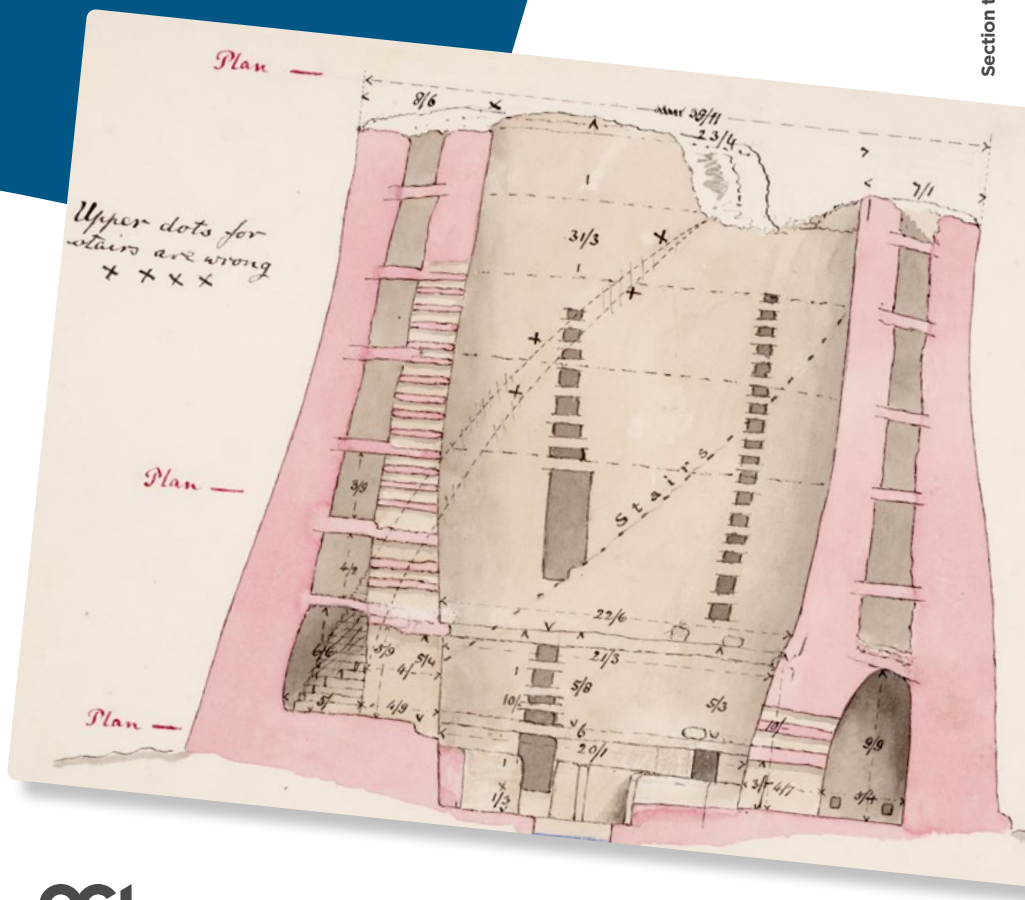
Digital content is increasingly the format for primary records, presenting new challenges for the preservation of our history. The HES Archives Digital Repository works to acquire, preserve and make accessible our digital collections.

Accessibility - Developing technologies means file formats, software and hardware often become inaccessible; we implement digital preservation techniques to combat obsolescence and ensure our historical digital collections can be continually accessed

Integrity - Digital collections are at risk of loss, corruption or unauthorised changes; we work within a robust digital preservation infrastructure to safeguard the integrity of our digital collections and ensure full intellectual control

Authenticity - Using metadata, we consider the lifecycle of our digital collections to preserve the context of their creation and therefore ensure their provenance, veracity and trustworthiness

> To preserve, conserve and develop our collections



Section through Broch of Mousa. ccanmore.org.uk/collection/1365543

HISTORIC ENVIRONMENT SCOTLAND | ÀRAINNEACHD EACHDRAIDHEIL ALBA

Historic Environment Scotland
John Sinclair House
16 Bernard Terrace
Edinburgh EH8 9NX

T. 0131 662 1456
E: Digital.Archives@hes.scot
www.canmore.org.uk
@HistEnvScot

Scottish Charity No: SCO45925
VAT Number: GB 221 8680 15