



National Library of Scotland OAIS Archive

Notes Before Completing the Application

We have read and understood the notes concerning our application submission.

True

Reviewer Entry

Reviewer 1

Comments:
accept

Reviewer 2

Comments:

CORE TRUSTWORTHY DATA REPOSITORIES REQUIREMENTS

Background & General Guidance

Glossary of Terms

BACKGROUND INFORMATION

Context

R0. Please provide context for your repository.

Repository Type. Select all relevant types from:

National repository system; including governmental, Publication repository, Library, Archive

Reviewer Entry

Reviewer 1

Comments:
accept

Reviewer 2

Comments:
accept

Brief Description of Repository

Please refer to the glossary [R0.1] for terms used in this application.

The National Library of Scotland is a national institution governed by statute [R0.2]. It is the foremost reference library in Scotland and its only legal deposit library [R0.3]. The National Library of Scotland has a legal obligation to collect, catalogue, index, archive and make available collections relevant to Scotland. These collections include, but are not limited to, digital and physical forms of books, maps, other print publications, web sites, business records, social media, sheet music, audio recordings, film & video recordings, and archives. It also creates new digital collections through an active digitisation programme that has been running for over 20 years. The scope and breadth of its collections will change with time, as new formats and technologies become available. The National Library of Scotland's website provides more details of its mandate, function, services, and strategic commitment to safeguarding access to its collections [R0.4-0.5].

The Library, hereafter referred to as the Repository, has an OAIS Archive containing a digital subset of Collections and Archived Business Records as described in the Digital Preservation Content Register [R0.6]. This excludes its non-print (i.e. digital) legal deposit collections, developed through a legal privilege to claim a copy of anything published in the UK, which are jointly managed by the UK Legal Deposit Libraries.

The OAIS Archive is managed by the Repository's Digital Preservation Team, supported by its IT and Development teams, governed by a Repository-wide Digital Preservation Steering Group and cognisant of its two main designated communities: "Content Group Controllers" and "Web Users". Each community, in conjunction with the data in the OAIS Archive, direct the development of the OAIS Archive within the operational constraints set by the Repository's Leadership Team and overseen by the Repository's Digital Preservation Steering Group.

To give a sense of scale the Repository has a staff of 271 full-time equivalents, and web services that are used through 7 million sessions per year. The OAIS Archive manages 46 million files amounting to 655TB of data per copy and provides this to the "Content Group Controllers" designated community. Although half of the files cannot be made directly accessible to the public, web-friendly versions of digitised collections that represent the vast majority of this data are publicly available to the "Web Users" designated community through the Repository's web services.

The Library, hereafter referred to as the Repository, has an OAIS Archive containing a digital subset of Collections and Archived Business Records as described in the Digital Preservation Content Register [R0.4]. This excludes its non-print (i.e. digital) legal deposit collections, developed through a legal privilege to claim a copy of anything published in the UK, which are jointly managed by the UK Legal Deposit Libraries.

The OAIS Archive is managed by the Repository's Digital Preservation Team, supported by its IT and Development teams, governed by a Repository-wide Digital Preservation Steering Group and cognisant of its two main designated communities: "Content Group Controllers" and "Web Users". Each community, in conjunction with the data in the OAIS Archive, direct the development of the OAIS Archive within the operational constraints set by the Repository's Leadership Team and overseen by the Repository's Digital Preservation Steering Group.

Reviewer Entry

Reviewer 1

Comments:
accept

Reviewer 2

Comments:
accept

Brief Description of the Repository's Designated Community.

The OAIS Archive serves two designated communities:

"Content Group Controllers" are the members of Repository staff responsible for various Collections and Archived Business Records, referred to as "Content Groups", that are provided to the OAIS Archive to safeguard and ensure long-term access to the content. Content Group Controllers have the authority to make decisions about the Content Groups they are responsible for including who has access, if data can be changed, and how long the data should be kept in the OAIS Archive. They also act as the contact point for OAIS Archive Staff.

"Web Users" are members of the public and Repository staff who access content from the OAIS Archive through public websites managed by the Repository. Web Users must have internet access and sufficient skills to interact with browser-based web services written in English and using text, images, and maps as the main navigational aids. Beyond these limits, web services are intentionally aimed at a broad audience, and used by people from around the world. Only Content Groups where the Repository has permission and the ability to deliver in this way are available, and Web Users see a copy of the data transformed to suit the web service they use. The OAIS Archive plays an active role in controlling access and communicating what permissions apply to the content in its care.

Reviewer Entry

Reviewer 1

Comments:

accept

Reviewer 2

Comments:

accept

Level of Curation Performed. Select all relevant types from:

B. Basic curation – e.g. brief checking; addition of basic metadata or documentation, C. Enhanced curation – e.g. conversion to new formats; enhancement of documentation, D. Data-level curation – as in C above; but with additional editing of deposited data for accuracy

Reviewer Entry

Reviewer 1

Comments:

accept

Reviewer 2

Comments:

accept

Comments

The OAIS Archive manages different Content Groups with different levels of curation as agreed with the Content Group Controller. Levels of curation are described in the Digital Preservation Content Register for each Content Group. All content has some level of curation (CoreTrustSeal levels B, C and D), and some content may be adjusted or replaced. As an illustration:

An interview is always conducted with each Content Group Controller to find out more about the content, e.g. rights, risks, and requirements for access. In 2021-2022 the Repository will ensure all Content Groups have a full Digital Preservation and Access Plan recorded in the Digital Preservation Content Register to complement the original interview.

On ingest, fixity checks are made, and persistent IDs and paths are assigned. This is all recorded as new metadata.

For content where authenticity is not important the OAIS Archive can, within an appropriate governance and quality control structure, change the formats of the files or correct them without retaining the originals. This has allowed the Repository to switch to more beneficial preservation formats for images and AV material created through its digitisation programme.

Technical metadata improvements are made to all Content Groups and descriptive metadata improvements are made to Content Groups relating to the digitisation of visual and textual material. In both examples the improved metadata is held separately to the original deposit.

Reviewer Entry

Reviewer 1

Comments:
accept

Reviewer 2

Comments:
accept

Insource/Outsource Partners. If applicable, please list them.

Amazon Web Services

- Nature of relationship: Commercial Contract

- Used for: Storing a 3rd distinct copy of preservation data and serving a public copy of some content to the "Web Users" designated community

- Qualifications/ certifications: <https://aws.amazon.com/compliance/programs/>

Ex Libris

- Nature of relationship: Commercial Contract

- Used for: Alma [R0.7] and Primo [R0.8] products that display online catalogue records with links to some public content for the "Web Users" designated community.

- Qualifications/ certifications: Alma conforms to FERPA [R0.9] guidelines to protect user data. Alma and Primo achieve FedRAMP Tailored Authorization for cloud security. Ex Libris have achieved ISO 27001 certification for security of information systems. The Ex Libris standard SLA commitment is to deliver service availability of at least 99.5%, measured over any calendar year and they publish uptime reports, and Root-Cause-Analysis reports for downtime events.

Reviewer Entry**Reviewer 1**

Comments:
accept

Reviewer 2

Comments:
accept

Summary of Significant Changes Since Last Application (if applicable).

This is the National Library of Scotland's first application.

Reviewer Entry

Reviewer 1

Comments:
accept

Reviewer 2

Comments:
accept

Other Relevant Information.

A Compliance Level of 3 is used to indicate that almost all of a requirement has been fully implemented and a few sub-requirements will be fully implemented within 18 months as detailed in the response to the requirement.

The applicant has provided a Glossary of abbreviations of terms that readers may be unfamiliar with. It is listed once, as Supporting Evidence of Requirement 0, although it is useful for the whole application [R0.1].

This application uses the definitions in the CoreTrustSeal Glossary with the following deviations and additions, some of which are shown in Figure 1:

- The CoreTrustSeal Glossary definitions of Archive, OAIS, and OAIS Archive are brought under the umbrella term OAIS Archive.
- The applicant defines the term Content Group to describe groups of preservation data that are controlled by the same member of staff and have similar characteristics that allow them to be managed in the same way.
- The applicant defines the term Content Group Controllers as the members of staff responsible for specific Content Groups. This is separate to OAIS Archive staff who manage the content on behalf of the Content Group Controllers. A fuller definition is provided above under Designated Communities.
- The applicant does not currently have an example where Producers outside of the Repository directly add content to the OAIS Archive. All additions are mediated through members of Repository staff who prepare and provide the content to the OAIS Archive. Therefore, a distinction is made between External Producers and Internal Producers with the term data producers, used frequently in the CoreTrustSeal guidance, used by the applicant as a substitute for Internal Producers.

Figure 1: Visual context and definitions for the National Library of Scotland's OAIS Archive

<https://doi.org/10.34812/T4DM-HY93>

SUPPORTING EVIDENCE

R0.1) Glossary

<https://doi.org/10.34812/z2dh-0718>

R0.2) re3data.org registry entry for the National Library of Scotland

<https://www.re3data.org/repository/r3d100013589>

R0.3) Legal deposit at the National Library of Scotland:

<https://www.nls.uk/about-us/legal-deposit/>

R0.4) About the National Library of Scotland:

<https://www.nls.uk/about-us/what-we-are/>

R0.5) National Library of Scotland strategy:

<https://www.nls.uk/media/43mla4h3/2020-2025-library-strategy.pdf>

R0.6) Example records in the Digital Preservation Content Register:

<https://doi.org/10.34812/8b0t-e697>

R0.7) Alma

<https://exlibrisgroup.com/products/alma-library-services-platform/>

R0.8) Primo

<https://exlibrisgroup.com/products/primo-discovery-service/>

R0.9) FERPA

<https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html>

Reviewer Entry

Reviewer 1

Comments:

accept

Reviewer 2

Comments:

accept

ORGANIZATIONAL INFRASTRUCTURE

1. Mission/Scope

R1. The repository has an explicit mission to provide access to and preserve data in its domain.

Compliance Level:

4 – The guideline has been fully implemented in the repository

Reviewer Entry

Reviewer 1

Comments:

4 – The guideline has been fully implemented in the repository accept

Reviewer 2

Comments:

4 – The guideline has been fully implemented in the repository accept

Response:

At the National Library of Scotland we are committed to the mission, vision and guiding principles set out in our 2020-2025 strategy. [R1.1]

The National Library of Scotland Act 2012, the Legal Deposit Libraries Act 2003, and the Legal Deposit Libraries (Non-Print Works) Regulations 2013 gives the Repository the legal mandate to collect, safeguard and provide access to its collections [R1.2-1.4]. This mandate can be traced back to the National Library of Scotland 1925 Act and the Repository's collections have grown in size and scope since with an increasing amount of digital content.

The Repository's Archived Business Records are managed in accordance with the Public Records (Scotland) Act 2011 [R1.5] to ensure their authenticity, reliability, integrity, and usability.

The Repository's mandate for preservation and access are reflected in "Reaching People: Library Strategy 2020-2025" [R1.6].

- A programme of preservation and digitisation of moving image and sound will save some of the most fragile formats in the country from disintegration. A project will be developed to preserve, digitise and make available to the nation Scotland's newspaper heritage. (p.2)

- We will collect, preserve and make available diverse materials that represent the lives and memories of Scotland's people, and which contribute to world knowledge. (p.10)

- People will have access to more than 10 million of the Library's items in digital format as we complete our 'One Third

Digital' initiative. (p.13)

The Repository has been digitising its collections for over 20 years and digitisation has been a cornerstone of successive strategies that have helped to preserve physical originals and provide unprecedented levels of access to a global audience. The Repository has a business need and public duty to protect this investment.

The Library Leadership Team oversees a published Digital Preservation Policy and Plan [R1.7] that ensures ongoing access to the digital content the Repository is responsible for preserving. It falls upon the OAIS Archive to execute the policy under the direction of the Digital Preservation Steering Group [R1.7 section 3.1].

It is important to state that the Repository does not want to preserve all digital content it has - some is ephemeral, some is intentionally destroyed e.g. as part of Records Management procedures, and some can be automatically derived from other sources. What we currently collect is detailed in our Collection Development Policy. [R1.8]

SUPPORTING EVIDENCE

R1.1) The National Library of Scotland's mission, vision, and values

<https://www.nls.uk/about-us/what-we-are/our-mission/>

R1.2) National Library of Scotland Act 2012:

<http://www.legislation.gov.uk/asp/2012/3/contents/enacted>

R1.3) Legal Deposit Libraries Act 2003:

<https://www.legislation.gov.uk/ukpga/2003/28/contents>

R1.4) Legal Deposit Libraries (Non-Print Works) Regulations 2013:

<https://www.legislation.gov.uk/uksi/2013/777/made>

R1.5) Public Records (Scotland) Act 2011:

<https://www.legislation.gov.uk/asp/2011/12/contents>

R1.6) National Library of Scotland strategy:

<https://www.nls.uk/media/43mla4h3/2020-2025-library-strategy.pdf>

R1.7) Digital Preservation Policy and Plan:

<https://doi.org/10.34812/a77g-j261>

R1.8) Collection Development Policy

<https://doi.org/10.34812/gpde-cw03>

Reviewer Entry

Reviewer 1

Comments:
accept

Reviewer 2

Comments:
accept

2. Licenses

R2. The repository maintains all applicable licenses covering data access and use and monitors compliance.

Compliance Level:

4 – The guideline has been fully implemented in the repository

Reviewer Entry

Reviewer 1

Comments:
4 – The guideline has been fully implemented in the repository
accept

Reviewer 2

Comments:
4 – The guideline has been fully implemented in the repository
accept

Response:

The Repository provides clear guidance to its designated communities about the requirements of content licenses and the actions the Repository will take for non-compliance [R2.1-R2.2]. Much of the digital content published online may be re-used for commercial and non-commercial purposes without a content licence, as indicated by any rights statement or licence applied. This is typically a Creative Commons license statement on the web page containing the digital content. Details on third party rights to re-use Library material and how to apply for special licenses are given on the National Library of Scotland website. [R2.3]

Complementing this is a published Metadata and Digital Content Licensing Policy [R2.4] with definitions, procedures, and guidance for the licensing of digital content created or owned by the Repository. This is due to be replaced by a Re-use Policy in 2021-22.

Licensing and compliance are managed by the Rights and Information Manager and Information Officer. They also

manage commercial licenses, contractual agreements, and data protection and privacy legislation that apply to the data within the Repository's OAIS Archive and influence licensing to others. The OAIS Archive manages groups of content ("Content Groups") and records information that may inhibit their re-use and licensing in the Digital Preservation Content Register. For some Content Groups additional metadata may be recorded in the Digital Preservation Database (known in the Library as the Digital Object Database or DOD) to control re-use and licensing at file level.

Non-compliance of terms by Repository staff could lead to disciplinary measures, including dismissal. Measures applicable for breaches of the terms of public access are detailed on the National Library of Scotland website [R2.5], in addition to those mentioned in the content license.

SUPPORTING EVIDENCE

R2.1) Content License information:

<https://www.nls.uk/using-the-library/copying-services/permission/licence>

R2.2) Content License:

<https://doi.org/10.34812/pw45-3x18>

R2.3) Permission to re-use Library material

<https://www.nls.uk/using-the-library/copying-services/permission/>

R2.4) Metadata and Digital Content Licensing Policy:

<https://doi.org/10.34812/4p74-5t62>

R2.5) Breaches of terms and conditions of use Library facilities, services and collections:

<https://www.nls.uk/using-the-library/terms-and-conditions/breaches>

Reviewer Entry

Reviewer 1

Comments:

accept

Reviewer 2

Comments:

accept

3. Continuity of access

R3. The repository has a continuity plan to ensure ongoing access to and preservation of its holdings.

Compliance Level:

3 – The repository is in the implementation phase

Reviewer Entry

Reviewer 1

Comments:

4 – The guideline has been fully implemented in the repository accept

Reviewer 2

Comments:

4 – The guideline has been fully implemented in the repository accept

Response:

RESPONSIBILITY AND PRESERVATION PERIODS

Preservation periods for Collection content is set by the Content Group Controller and tends to be "in perpetuity".

The preservation period for Archived Business Records is dictated by the Business Classification and Retention Scheme [R3.1]. An exception is made to preserve Archived Business Records sooner if they relate to other content in the Repository's OAIS Archive e.g. a commercial contract with an embargo period that is related to digitised images in the OAIS Archive.

All content is deposited after a Digital Preservation and Access Plan has been agreed by the Content Group Controller and the Repository. This is recorded in the Digital Preservation Content Register with information about the Content Group deposited, including the preservation period, and the responsibilities of the Content Group Controller and Repository.

MEDIUM AND LONG-TERM CONTINUITY OF ACCESS

Established in 1925 under legal statute, with an amended National Library of Scotland Act in 2012 [R3.2], the National Library of Scotland is a national institution with core obligations to safeguard and make available its collections. Any change of stewardship or function would require a change in the law and there is no indication that its core functions are under threat from any social, economic, or political changes.

More likely are changes in legislation to merge bodies with their core functions and data holdings left intact. In this way the Historic Environment Scotland Act 2014 merged Historic Scotland with the Royal Commission on the Ancient and Historical Monuments of Scotland, and the National Records of Scotland resulted from the merger of the General Register Office for Scotland with the National Archives of Scotland in 2011. For such events there are 3 points to make for the Repository:

1) Our active preservation planning, and knowledge and management of the data prepares us for changes in systems, storage and data processing that will assist in large scale changes affecting the Repository. Mergers typically last several years from first knowledge to full implementation and the Repository can confidently make changes within this period.

2) The Repository is allowed to transfer most of the data in its OAIS Archive to another organisation. Existing agreements for some data may not permit this and there is a risk that parties to those agreements will not allow the data to be transferred to the new organisation. In such cases, the Repository would use its best endeavours to negotiate new agreements to transfer content to another organisation. For any content that cannot be transferred the Repository accepts this risk and can easily identify and remove the affected content.

3) The new organisation may change or not meet the preservation and access commitments formerly set by the National Library of Scotland (the Repository).

Other risks to continuity and the Repository's plans to mitigate them are described in the Digital Preservation Risk Register and overseen by the Digital Preservation Steering Group, itself created by and reporting to the Library Leadership Team.

SUPPORTING EVIDENCE

R3.1) NLS Business Classification and Retention Scheme:

<https://doi.org/10.34812/h29j-hr07>

R3.2) National Library of Scotland Act 2012:

<http://www.legislation.gov.uk/asp/2012/3/contents>

Reviewer Entry

Reviewer 1

Comments:

accept

Reviewer 2

Comments:

accept

4. Confidentiality/Ethics

R4. The repository ensures, to the extent possible, that data are created, curated, accessed, and used in compliance with disciplinary and ethical

norms.

Compliance Level:

4 – The guideline has been fully implemented in the repository

Reviewer Entry

Reviewer 1

Comments:

4 – The guideline has been fully implemented in the repository
accept

Reviewer 2

Comments:

4 – The guideline has been fully implemented in the repository
accept

Response:

The Repository's OAIS Archive contains a mix of Archived Business Records and Collection content, some of which contain personal and sensitive data.

POLICY FRAMEWORK

Disclosure risk for the Repository is controlled by the Data Protection Policy [R4.1] that covers the majority of Requirement 4, including managing and controlling sensitive data and risk, compliance with legislation, enforcement, and training. Data Protection is managed by the Rights and Information Manager (as Data Protection Officer), and the Information Officer. Key excerpts from the Data Protection Policy are:

- The policy applies to all personal data processing activities carried out by the National Library of Scotland or on behalf of the Library. The Library, its employees and agents shall not process personal data except in accordance with the principles relating to processing of personal data in Article 5 of the General Data Protection Regulation (GDPR) or as otherwise permitted in the Data Protection Legislation [R4.1 Section 2.1].
- The Library will maintain and keep up to date a record of personal data processing activities by means of the Personal Data Register [R4.1 Section 7.1]. Processing is reviewed by the Library's Data Protection Officer.
- The Library will conduct a data protection impact assessment prior to the processing of personal data likely to result in a high risk to the rights and freedoms of individuals [R4.1 Section 17.1].
- The Library will prepare and maintain appropriate processes, procedures, and guidance in relation to processing of personal data for archiving, research, statistical, and freedom of expression purposes, noting that such have a particular

pertinence to the Library's core aims and objectives [R4.1 Section 21.1].

- The Library will provide suitable training and support in matters of data protection for all employees [R4.1 Section 23].
- Personal data processed by the Library must be managed in accordance with the Information Security Policy [R4.2], the Records Management Plan [R4.3], and the Library's other information, data, and property security policies and procedures [Ref 4.1 Section 15.1].

The Repository deals with ownership, due diligence and restitution of material as stated in its Collection Development Policy [R4.4]:

- The Library acquires material legally, ethically and with due diligence. The Library will always do its utmost to confirm that the vendor or donor has proper title to the item offered to the Library. The Library will cooperate with relevant bodies and organisations with regard to any claims of restitution, and consider the evidence. We will assist the authorities with restitution of cultural items according to UNESCO guidance. We refer to and recognise relevant professional guidance on ethics and building diverse collections in our collection development activities, for example, the International Federation of Film Archives (FIAF) Code of Ethics [R4.4 Section 4.3].

The Repository's Takedown Policy [R4.5] provides a mechanism to remove material on the grounds of copyright infringement, sensitive and personal data breaches, or obscene or defamatory content.

Finally, the Repository explains how it processes the personal data of suppliers of collection content, including that in its OAIS Archive [R4.6].

ASSESSING AND CONTROLLING COLLECTION RISK

Within this policy framework Repository staff evaluate content for copyright, contractual, and sensitive information prior to passing it to the OAIS Archive for ingest. This information is recorded in Collection Impact Assessments, collection catalogues, and donation, deposit and vendor agreements. In the OAIS Archive sensitivity concerns are recorded in the digital preservation database, and the Digital Preservation Content Register to control the use of Content Groups beyond that provided to Content Group Controllers [R4.7].

The OAIS Archive also allows additional information to be added or existing information updated after ingest e.g. if individual files have different data protection requirements within the Content Group, or if better information becomes available.

Work is ongoing to create a Sensitivity Review Framework to standardise Repository practice used to assess collections for sensitive information. The aim is to complete this in 2021-22.

SUPPORTING EVIDENCE

R4.1) Data protection policy:

<https://doi.org/10.34812/80wy-c205>

R4.2) Information security policy:

<https://doi.org/10.34812/yhye-x905>

R4.3) Records Management Plan:

<https://doi.org/10.34812/1rfh-wq15>

R4.4) Collection Development Policy:

<https://doi.org/10.34812/gpde-cw03>

R4.5) NLS Takedown policy:

<https://doi.org/10.34812/qwye-r369>

R4.6) Acquisition and loans privacy notice:

<https://www.nls.uk/privacy/acquisitions-and-loans-notice>

R4.7) Example records in the Digital Preservation Content Register:

<https://doi.org/10.34812/8b0t-e697>

Reviewer Entry

Reviewer 1

Comments:

accept

Reviewer 2

Comments:

accept

5. Organizational infrastructure

R5. The repository has adequate funding and sufficient numbers of qualified staff managed through a clear system of governance to effectively carry out the mission.

Compliance Level:

4 – The guideline has been fully implemented in the repository

Reviewer Entry

Reviewer 1

Comments:

4 – The guideline has been fully implemented in the repository
accept

Reviewer 2

Comments:

4 – The guideline has been fully implemented in the repository
accept

Response:

ORGANISATIONAL STABILITY

The National Library of Scotland (the Repository) was formally constituted by an Act of Parliament in 1925 and was built on the de facto 'national library' of the Faculty of Advocates, which was founded in the 1680s and had been Scotland's only legal deposit library since 1710. It is now one of the major research libraries in Europe and the responsibility of the Scottish Government after the passing of the National Library of Scotland Act 2012 [R5.1]. At its core is the responsibility to acquire, safeguard and make available its collections. Any change of stewardship or function would require a change in the law and there is no indication that this is under threat from any social, economic, or political changes.

The Repository gets most of its funding from the Scottish Government as Grant in Aid, with additional income from donations, charitable activities, investments, and trading activities. As an illustration income for the three financial years of 2017/18, 2018/19, and 2019/20 has been £19.9M, £17.1M, and £17.8M respectively. For the last decade Government funding has been allocated on an annual basis. This introduces uncertainty for the Repository's mid to long-term financial planning but in practice funding has been consistent over time with additional support for capital projects, some of which benefit the Repository's OAIS Archive. Annual Reviews are published online to provide details of Repository funding going back to 1997 [R5.2].

The combination of funding and legal statute provides the Repository with confidence that its OAIS Archive will exist long-term. This is supported by an internal commitment from the Repository's Library Leadership Team to fund sufficient storage for digital collections including those that are on legacy digital and analogue media. More granular preservation costs for data in the Repository's OAIS Archive will be provided over time including an assessment in 2021-23 of Content Groups that may need to be preserved in the future. They include legacy content in the Repository's Archived Business Records; archives managed by the Manuscripts team; digital legal deposit content; and digital content on legacy media in Modern Collections [R5.3 Section 3.2.3].

GOVERNANCE AND STAFF

The Repository has a Digital Preservation Policy and Plan [R5.3], and its digital preservation activity and OAIS Archive is governed by the Library Leadership Team and the Digital Preservation Steering Group [R5.3, Section 3.1.2 and R5.4] that ensure the delivery of the Repository's mission to safeguard and provide access to the content within it. The steering group has a membership that covers collections, business records, online services, rights, data protection, IT infrastructure, digitisation, and preservation.

They are complemented by a broader group of specialist practitioners responsible for application development, web content, digital ingest, digital collections, digital scholarship, networks, software systems, security, digital cataloguing & access, digital preservation etc. The skills of librarians, archivists, conservators, and traditional library disciplines are reflected in the extensive metadata that accompany our digital and digitised objects, and in the Digital Preservation and Access Plans drawn up with Repository staff. The Repository employs around 271 full-time equivalent staff.

The Repository has an Organisational Development Partner responsible for professional development and training of the Repository's staff with a dedicated budget and policy for this [R5.5]. The Repository is also an active member of various networks that benefit the Repository's mission and provide additional development opportunities for its staff. They include the International Federation of Library Associations and Institutions (IFLA), the International Internet Preservation Consortium (IIPC), the UK Web Archive (UKWA), the Archives and Records Association (ARA), the Digital Preservation Coalition (DPC), and the International Federation of Film Archives (FIAF).

SUPPORTING EVIDENCE

R5.1) National Library of Scotland Act 2012:

<http://www.legislation.gov.uk/asp/2012/3/contents>

R5.2) Annual Reviews and audited accounts:

<https://www.nls.uk/about-us/publications/annual-review>

R5.3) Digital Preservation Policy and Plan:

<https://doi.org/10.34812/a77g-j261>

R5.4) Digital Preservation Steering Group Terms of Reference:

<https://doi.org/10.34812/ca5c-ga48>

R5.5) Learning and Development Policy:

<https://doi.org/10.34812/yscz-tq67>

Reviewer Entry

Reviewer 1

Comments:
accept

Reviewer 2

Comments:
accept

6. Expert guidance

R6. The repository adopts mechanism(s) to secure ongoing expert guidance and feedback (either inhouse or external, including scientific guidance, if relevant).

Compliance Level:

4 – The guideline has been fully implemented in the repository

Reviewer Entry

Reviewer 1

Comments:
4 – The guideline has been fully implemented in the repository
accept

Reviewer 2

Comments:
4 – The guideline has been fully implemented in the repository
accept

Response:

To ensure the Repository is effective and relevant it consults a range of stakeholders and experts.

INTERNAL EXPERTS

The Repository's Library Leadership Team and Digital Preservation Steering Group govern digital preservation activity and the OAIS Archive, provide internal advice, and co-ordinate a programme of work for the Repository. The governors provide expertise in finance, human resources, strategy, collections, business records, service delivery, rights, data protection, IT infrastructure, digitisation, and digital preservation [R6.1, Section 3.1.2 and R6.2].

Expertise extends throughout the Repository's diverse workforce that can be called on to enable complex collections and projects to be managed successfully. The creation of Digital Preservation and Access Plans are done in conjunction with

the Content Group Controllers, frequently experts in the data they are submitting, and significant changes to the OAIS Archive will involve stakeholders from the planning process onwards.

EXTERNAL EXPERTS

The Repository's Digital Preservation Policy and Plan addresses its engagement of external experts [R6.1, Section 3.4] under the principle of Knowledge Transfer:

- We are an active member of the digital preservation community, engaging with others to meet shared challenges, and continually improving and developing the expertise and standards we require to preserve access to our content.

The examples given in the policy can be extended to include Library membership of the Scottish Cultural Heads of IT Services, involvement with the International Image Interoperability Framework (IIIF) community, international consultation in a 2020-21 Repository review of digital asset management systems, and formal and informal partnerships with heritage, cultural and research organisations. Furthermore, we are active members of the Digital Preservation Coalition on both its board and sub-committees.

DESIGNATED COMMUNITY FEEDBACK

The "Content Group Controller" designated community works collaboratively with the Repository's OAIS Archive to create Digital Preservation and Access Plans for their content. They are also consulted if changes to their plan are required, and they provide feedback about the Repository's ingest and access functions. This feedback is used to improve the Repository.

The "Web Users" designated community provide feedback in several ways through:

- Feedback links on pages with Repository content.
- General contact links on the Repository's websites.
- An annual Omnibus where 1000 participants are surveyed to test awareness of the Repository's services, user demographics, visitor behaviours, interests etc.
- User studies and comments when demonstrating or developing specific web services.

SUPPORTING EVIDENCE

R6.1) NLS Digital Preservation Policy and Plan:

<https://doi.org/10.34812/a77g-j261>

R6.2) Digital Preservation Steering Group Terms of Reference:

<https://doi.org/10.34812/ca5c-ga48>

Reviewer Entry

Reviewer 1

Comments:
accept

Reviewer 2

Comments:
accept

DIGITAL OBJECT MANAGEMENT

7. Data integrity and authenticity

R7. The repository guarantees the integrity and authenticity of the data.

Compliance Level:

4 – The guideline has been fully implemented in the repository

Reviewer Entry

Reviewer 1

Comments:
4 – The guideline has been fully implemented in the repository
accept

Reviewer 2

Comments:
4 – The guideline has been fully implemented in the repository
accept

Response:

FIXITY AND STOCK CHECKS

The Digital Preservation Data Integrity Policy [R7.1] describes how the Repository manages the integrity of data in its

OAIS Archive. In summary the OAIS Archive stores 3 distinct copies of data and makes the following commitments on fixity and stock checks:

- Known checksum values are obtained before the files are ingested and compared with the checksum values of each Distinct Copy to make sure file integrity is maintained at ingest.
- All files are fixity checked when file moves are controlled by the OAIS Archive.
- At least 2 copies are completely fixity checked once a year.
- A sample fixity check is made if the third copy is not completely fixity checked.
- Fixity check history is kept for all files and stored in a PREMIS compatible data structure.
- A stock-check of all copies will be made once a month from 2021-22.
- A diversification and distribution of risk for the 3 distinct copies gives the Repository confidence that unwanted changes detected during fixity and stock checks can be remedied with other copies.

COMPLETENESS

Content Group Controllers or their agreed representatives (data producers in OAIS terminology) provide folders containing data and metadata files for ingest into the OAIS Archive. OAIS Archive staff do not have permission to make changes to the ingest folders. At ingest the OAIS Archive creates a file listing of the supplied files with two checksums for each and uses this to confirm that all data has been successfully copied in duplicate (a third copy is made at a later date). During the ingest process additional metadata based on the PREMIS data dictionary is also created and stored in the Digital Preservation Database (known in the Library as the Digital Object Database or DOD), a Microsoft SQL Database created by the Repository to store metadata about digital files in preservation storage and managed by the Repository's OAIS Archive staff. The database uses several standards to structure and reference data and can be exported to satisfy many other standards. Staff and tools across the Repository add and update metadata. Data in the Digital Preservation Database includes:

- Pre-ingest path information.
- Current path information.
- A hierarchical structure of records including, for some Content Groups, descriptive records
- The relationships between different derivatives/representations of files for some Content Groups (e.g. an uncropped and

a cropped version of the same source image).

- MD5 and SHA-1 checksums (and a related creation and comparison event).
- A persistent identifier for each record in the descriptive, representation and file hierarchy.
- A variety of technical file information depending on file type including byte size, pixel dimensions, duration.

A receipt, that summarises the ingest process and lists the files ingested and metadata associated with them (including that listed above), is returned to the data producer to allow them to independently evaluate whether ingest was complete and successful, and to act as an audit trail to investigate the ingest process in the future. The OAIS Archive keeps a copy of the receipt.

Receipts are not created for the ingest of the "Library Digitised Still Image" Content Group because it uses a more automated ingest process that does not require management by OAIS Archive staff. Instead, digitisation staff confirm the completeness of data and metadata by running a series of queries against the Digital Preservation Database. Future improvements to the tool may automate this step too.

CHANGES TO DATA AND METADATA, AND VERSIONING

Changes to metadata related to the files in the OAIS Archive can be made in collection databases (for moving image and electronic manuscript Content Groups) and the Digital Preservation Database (for all Content Groups) as per Box 1 & 2 in Figure 2. Controls are in place to restrict the staff who can update the metadata and multiple database logs and back-ups are maintained to allow unwanted changes to be rolled back as per Box 3 in Figure 2. In 2021-2022 the Repository will investigate ways to improve the management of metadata integrity independently of collection databases and systems, including the use of specifications such as Oxford Common File Layout to manage the versioning of metadata (Figure 2, Box 4b).

Figure 2: The location of metadata for content in the Repository's OAIS Archive:

<https://doi.org/10.34812/dan8-5421>

It is important to note that changes to any form of metadata or data in preservation storage (Figure 2, Box 4) in the OAIS Archive is not permitted as standard as defined by the Digital Preservation Data Integrity Policy. In essence:

- No delete permissions are provided for any copies of data in preservation storage and can only be temporarily granted with the Digital Preservation Steering Group's oversight and authorisation.
- The use of versioning prevents accidental or malicious replacement of previous versions with new bad versions.

- All overwrites require appropriate levels of approval and this information is recorded by OAIS Archive staff, and previous versions are retained.

All ingest tools for all Content Groups identify potential overwrites and require a manual overwrite request. An approved overwrite request is recorded in the standard ingest receipt with one copy of the receipt retained by the OAIS Archive and one returned to the data producer. In addition, PREMIS overwrite events with new checksum information and data producer details are recorded in the Digital Preservation Database. If requested, OAIS Archive staff share technical file information with the data producer to allow them to make comparisons between the incoming and archived file before they request an overwrite. This includes checksum, byte size, and pixel dimension information. Exact duplicates are not ingested.

AUTHENTICITY

The Repository deals with ownership, due diligence and restitution of material as stated in its Collection Development Policy and acquires material legally, ethically and with due diligence. The Repository will always do its utmost to confirm that the vendor or donor has proper title to the item offered to the Library [R7.2 Section 4.3].

With very few exceptions the Repository owns the data in its OAIS Archive. The Repository is permitted to change the data to ensure it is safe and accessible in accordance with legislation and contractual agreements. In addition, the OAIS Archive describes how changes to the data are managed, including any contractual controls, by creating a Digital Preservation and Access Plan for each Content Group with the Content Group Controller. The Content Group Controller is a member of Repository staff and acts as the internal data producer.

During the creation of the Digital Preservation and Access Plan any need to demonstrate the authenticity of the Content Group will be identified. If so, additional provenance information may be required, and the data must be able to be returned to the Content Group Controller exactly as provided to the Repository's OAIS Archive with information about the content's integrity since receipt and any changes enacted on the data. Returning data as supplied permits a limited set of reversible changes, but often the data will be preserved at bit-level as supplied and future access requirements may lead to the creation of additional, alternative derivatives. The Digital Preservation and Access Plans are recorded in the Digital Preservation Content Register and an example of a Content Group with an authenticity requirement is provided as supporting evidence [R7.3].

Supporting Evidence:

R7.1) Digital Preservation Data Integrity Policy:

<https://doi.org/10.34812/173d-f765>

R7.2) Collection Development Policy:

<https://doi.org/10.34812/gpde-cw03>

R7.3) Example records in the Digital Preservation Content Register:

<https://doi.org/10.34812/8b0t-e697>

Reviewer Entry

Reviewer 1

Comments:
accept

Reviewer 2

Comments:
accept

8. Appraisal

R8. The repository accepts data and metadata based on defined criteria to ensure relevance and understandability for data users.

Compliance Level:

4 – The guideline has been fully implemented in the repository

Reviewer Entry

Reviewer 1

Comments:
4 – The guideline has been fully implemented in the repository
accept

Reviewer 2

Comments:
4 – The guideline has been fully implemented in the repository
accept

Response:

DATA SELECTION AND APPRAISAL

The Repository has a comprehensive and detailed Collection Development Policy [R8.1] that includes appraisal criteria for the selection of collection content. Any digital collection material retained or created by the Repository will be added to its OAIS Archive and rights are obtained to allow this.

Section 5.2 of the policy details the key collection areas of focus. Other sections of note for digital content in the Repository's OAIS Archive are:

- We take into account access, metadata, storage, digitisation and preservation requirements for physical and digital formats. We will assess and advise, where this is an option, on how best to provide the Library with digital formats. (Section 3, para. 4)
- For digital materials such as interactive e-books, we may additionally collect relevant hardware, software, licences or other dependencies that help maintain the full functionality of the content. (Section 4.6, para. 3)
- The Library monitors developments in emerging formats, particularly digital. It will adopt new formats where appropriate. (Section 4.11, para. 2)
- Where the Library does not hold copies of the originals, it aims to acquire or provide access to Scottish publications and other key works through surrogates, particularly digital. (Section 5.1.1, para. 16)
- The Library creates and selectively acquires data derived from its collections and collection items, and contextual supporting data. (Section 5.3, 'Data').
- We reserve the right to decline material, or remove access to it on the grounds of illegal content, intellectual property infringements, or risk to the collections or staff. (Section 4.4, para. 4)

Digital collections acquired under non-print legal deposit legislation are managed by a joint legal deposit library infrastructure and is outside of the scope of this CoreTrustSeal application.

The Repository uses a Business Classification and Retention Scheme [R8.2] that describes which Business Records are live, which are to be destroyed, and which need to be archived in the OAIS Archive.

DATA AND METADATA ASSESSMENT/CHECKS

OAIS Archive staff and the Content Group Controller undertake a pre-preservation data quality assessment of the content that includes understanding its size, and identifying formats that are present and any risks to re-use by its designated community. OAIS Archive staff may reject some content if it is already in the OAIS Archive or there are insufficient funds to preserve it. The latter has not happened to date. OAIS Archive staff may also suggest that formats are changed, or additional ones created for preservation and re-use reasons. The assessment informs the creation of a Digital Preservation and Access Plan with the Content Group Controller for each Content Group in the OAIS Archive. Plans and the pre-preservation assessments are stored in the Digital Preservation Content Register [R8.3] and stipulate what

formats are allowed and what data and metadata are required to make the content understandable and accessible for their designated communities. The plan identifies who is responsible for the assessment of data and metadata, some of which will be automated. Responsibility is divided between the Content Group Controller or their agreed representatives (data producers), and OAIS Archive Staff. Examples of data and data quality criteria checked by the OAIS Archive Staff include:

- Re-use restrictions are provided
- Information is present to help designated communities understand the data as agreed
- Files are structured as agreed
- Supporting information files are restricted to certain formats
- Files will not supersede files already in the OAIS Archive without approval
- Business Classification and Retention Scheme numbers are supplied (for Archived Business Records)
- Files are supplied with other corresponding files or formats (for some content groups)
- Files do not already have descriptive records for an earlier copy (for some content groups)

If OAIS Archive Staff identify issues with data or metadata, they will work with the data producers to address them. Full Digital Preservation and Access Plans are in place for some Content Groups and will be complete for all Content Groups in 2021-22.

It is worth stating that Repository has complete control over formats for data and metadata for the digitised collections that make up the bulk of OAIS Archive data by volume. This has allowed the Repository to standardise formats and metadata for these Content Groups and use a variety of tools to create and ingest them with inbuilt quality control steps to ensure they meet agreed standards. Other collections and Archived Business Records, especially with authenticity requirements, provide less opportunity for the Repository to influence the original formats and are typically made accessible to the Content Group Controller as originally provided.

DATA REMOVAL

The Repository's policy is to retain the collections that it owns in perpetuity although in certain circumstances we may dispose of duplicates, redundant, unusable formats or items that pose a hazard to the collections or staff [R8.1 Section 4.4]. In practice the Repository makes it extremely difficult to delete data from its OAIS Archive as per the Digital Preservation Data Integrity Policy [R8.4] and requires the process to be documented and overseen by the Digital

Preservation Steering Group. Retention periods for all Content Groups are defined in the Digital Preservation Content Register.

Some Content Groups, including Collections and Archived Business Records, are added to the OAIS Archive with a limited retention period, e.g. if they are deposited in a temporary form and will be re-ingested in a final form in the future. As this content is not provided publicly the removal of these Content Groups and their persistent identifiers has no impact on access beyond the "Content Group Controller" designated community who requested their deletion.

Placeholder messages are used to inform the Web Users designated community if online content from the Repository is subject to a take-down request. The Repository is developing a persistent identifier framework that will include a response to handling deleted content. This work will be published in 2021-2022.

SUPPORTING EVIDENCE:

R8.1) Collection Development Policy:

<https://doi.org/10.34812/gpde-cw03>

R8.2) Business Classification and Retention Scheme:

<https://doi.org/10.34812/h29j-hr07>

R8.3) Example records in the Digital Preservation Content Register:

<https://doi.org/10.34812/8b0t-e697>

R8.4) Digital Preservation Data Integrity Policy:

<https://doi.org/10.34812/173d-f765>

Reviewer Entry

Reviewer 1

Comments:
accept

Reviewer 2

Comments:
accept

9. Documented storage procedures

R9. The repository applies documented processes and procedures in managing archival storage of the data.

Compliance Level:

4 – The guideline has been fully implemented in the repository

Reviewer Entry

Reviewer 1

Comments:

4 – The guideline has been fully implemented in the repository
accept

Reviewer 2

Comments:

4 – The guideline has been fully implemented in the repository
accept

Response:

High level descriptions of how we manage archival storage of data is detailed by the Repository's Digital Preservation Policy and Plan [R9.1]. More detail is provided in the Digital Preservation Data Integrity Policy [R9.2]. Procedures and workflows for ingest (that include data quality requirements), storage management and export of data for access are documented as part of the Digital Preservation and Access Plans drawn up for each Content Group [R9.3] and as a centralised Digital Preservation Workflows document [R9.4]. Documentation is managed by the Repository's Digital Preservation team and referred to the Digital Preservation Steering Group when appropriate.

In summary, and with a focus on storage management, the Repository's OAIS Archive has:

- 3 distinct copies of preservation data.
- Two copies in 2 local and independent clouds in Edinburgh and Glasgow that replicate to each other. Both copies undergo an annual fixity check.
- A third copy in Amazon Deep Archive storage where a sample of files are annually fixity checked.
- System management tools in place to alert the Repository's IT infrastructure teams if there are issues with the hardware used for copies 1 and 2.
- The Digital Preservation Database (known as the Digital Object Database or DOD) to manage and maintain the location of copies 1 and 3. The location of copy 2 can be inferred from copy 1.
- A process to check copy 1, 2 and 3 for consistency.
- A process and history of annual fixity checks to provide a check for consistency between copies 1, 2, and the recorded path information in the Digital Preservation Database.

- A 2021-22 objective to start a monthly inventory check of all 3 copies and the Digital Preservation Database for improved security, consistency and service availability checks.

Risks associated with storage and data integrity are formally managed in the Digital Preservation Risk Register and overseen by the Digital Library Steering Group. Major risks to the data in the OAIS Archive are also the responsibility of the Library Leadership Team and included in the Library's Corporate Risk Register. Both risk registers use the Repository's Risk Management Framework [R9.5].

SUPPORTING EVIDENCE:

R9.1) Digital Preservation Policy and Plan:

<https://doi.org/10.34812/a77g-j261>

R9.2) Digital Preservation Data Integrity Policy:

<https://doi.org/10.34812/173d-f765>

R9.3) Example records in the Digital Preservation Content Register:

<https://doi.org/10.34812/8b0t-e697>

R9.4) Digital Preservation and Access Workflows:

<https://doi.org/10.34812/eamg-jq88>

R9.5) Risk Management Framework:

<https://doi.org/10.34812/8kcb-vz59>

Reviewer Entry

Reviewer 1

Comments:
accept

Reviewer 2

Comments:
accept

10. Preservation plan

R10. The repository assumes responsibility for long-term preservation and manages this function in a planned and documented way.

Compliance Level:

4 – The guideline has been fully implemented in the repository

Reviewer Entry

Reviewer 1

Comments:

4 – The guideline has been fully implemented in the repository accept

Reviewer 2

Comments:

4 – The guideline has been fully implemented in the repository accept

Response:

The Repository uses a 3-tier preservation approach that links broad policy and plans to the practical management of groups of content and files within them.

- TIER 1: The Repository's Digital Preservation Policy and Plan [R10.1] is approved by the Library Leadership Team, overseen by the Digital Preservation Steering Group, and used by the Repository's OAIS Archive. Progress against the plan is measured and monitored by the Digital Preservation Steering Group to help ensure actions are completed [R10.2].

- TIER 2: The Digital Preservation Content Register [R10.3] stores Digital Preservation and Access Plans for each Content Group in the Repository's OAIS Archive. The plans act as an agreement between the Content Group Controller (a member of staff responsible for specific Content Groups) and the OAIS Archive. The responsibilities of both parties are clearly defined. The plan records information such as data provenance and risk (including obsolescence) and outlines the Repository's commitments to make the content understandable and accessible to a designated community for a specified period.

With very few exceptions the Repository is the owner of the content in the OAIS Archive and has the right to manage the data in order to meet the commitments outlined in the plan. On rare occasions, limits, such as embargo periods for public access, may be imposed by a depositor agreement, a contract with the content supplier, rights owner, or standing obligations and restrictions. The Repository will actively preserve such contracts and/or metadata to describe how use is restricted but in all cases the Repository obtains sufficient permission to preserve the content.

- TIER 3: The Digital Preservation Database records information about individual files in the Content Groups to help manage them over time.

General risks identified in the Digital Preservation and Access Plans are copied to the Digital Preservation Risk Register and managed there by OAIS Archive staff with oversight from the Digital Preservation Steering Group. This includes risks of obsolescence and it is worth noting two related pieces of work that are planned for the Repository:

- A long-term aim is to identify the software required to render the files in its OAIS Archive (2021-2023), in particular for legacy formats, in order to create a software library/registry.

- A scoping study for data on legacy media that is not currently managed in the OAIS Archive. This is limited to Electronic Manuscripts, the Repository's Archived Business Records, and digital media included within Modern Collections (2021-2023).

The National Library of Scotland's digital preservation and access workflows are documented. [R10.4]

SUPPORTING EVIDENCE:

R10.1) NLS Digital Preservation Policy and Plan:

<https://doi.org/10.34812/a77g-j261>

R10.2) Digital Preservation Task Tracker:

<https://doi.org/10.34812/02gr-mp96>

R10.3) Example records in the Digital Preservation Content Register:

<https://doi.org/10.34812/8b0t-e697>

R10.4) Digital Preservation and Access Workflows

<https://doi.org/10.34812/eamg-jq88>

Reviewer Entry

Reviewer 1

Comments:
accept

Reviewer 2

Comments:
accept

11. Data quality

R11. The repository has appropriate expertise to address technical data and metadata quality and ensures that sufficient information is available for end users to make quality-related evaluations.

Compliance Level:

4 – The guideline has been fully implemented in the repository

Reviewer Entry

Reviewer 1

Comments:

4 – The guideline has been fully implemented in the repository
accept

Reviewer 2

Comments:

4 – The guideline has been fully implemented in the repository
accept

Response:

The Repository serves two main designated communities. They are Content Group Controllers, and Web Users, and this requirement is framed in response to their needs.

CONTENT GROUP CONTROLLERS

The Repository's OAIS Archive staff work with the Content Group Controller to assess data quality and risks, and agree a Digital Preservation and Access Plan for their Content Group(s) prior to ingest. The plan records what data and metadata are required to support use and understandability of the content for specific designated communities and what checks will be done by the Content Group Controller and the OAIS Archive.

The OAIS Archive uses one of several pre-ingest and ingest recipes suited to processing a particular Content Group. The recipes include a variety of data quality checks to make sure the data is supplied to the OAIS Archive as required. Checks are made of completeness, filenames, folder structures, formats, image sizes, pixel verification during AV and image conversions, partnering with sibling files, fixity, file size, and potential overwrites. Additional checks undertaken upstream by the Content Group Controller may also be undertaken including quarantined virus checks.

The ingest process is recorded in an ingest receipt. The OAIS Archive will contact the Content Group Controller or an agreed representative (as internal data producers) if issues, including of data quality, are detected and add this to the receipt. An ingest receipt is not created for the "Library Digitised Still Image" Content Group which has a more automated

series of checks managed by Digitisation staff.

Once any corrections are made and all checks are complete, files will be formally ingested to preservation storage and additional metadata will be added to the Digital Preservation Database in accordance with Repository standards, built largely on PREMIS. Database metadata includes original and archive file paths, structural relationships, agents, persistent identifiers, fixity information, and some technical file properties. A summary of the ingest process, including a full file listing, is added to the receipt and returned to the data producer.

After the initial ingest OAIS Archive staff create additional preservation metadata in the Digital Preservation Database to record format change events and regular fixity check events, and undertake regular stock checks [R11.1]. This can be used by the designated community to assess the integrity and authenticity of the data and confirm that the data quality at ingest persists. Furthermore, the Repository reacts to any issues in metadata or access identified by the designated community.

To reference data in the OAIS Archive the Designated Community uses path information, and NLS DOD (National Library of Scotland Digital Object Database) persistent identifiers that use an internal scheme, minter and resolver managed by the Repository.

The combination of a Digital Preservation and Access Plan, the information in the ingest receipt, and metadata in the Digital Preservation Database enables the Content Group Controller designated community to evaluate the quality of the data.

WEB USERS

This designated community uses a variety of web services to access an exported subset of content, namely digitised versions of physical collections, stored in the Repository's OAIS Archive. Data quality checks were made at ingest, and further checks are made at publication to ensure the web services have the information required, for example that a collection of content is complete and appropriately structured. The Repository provides these services and a range of metadata to help people understand and evaluate the content. This includes descriptive, technical, structural and contextual information, and the Repository explains how people can re-use the content. An exemplar web service is the Data Foundry [R11.2] that provides additional context about the quality, scope, and provenance of the data provided.

Citations to the content are supported through permanent URLs on many of the web service pages which also allow the designated community to provide feedback. Permanent URLs use a combination of DOI persistent identifiers, NLS DOD persistent identifiers and, for the moving image web service, system IDs with the potential to become persistent through a Repository review in 2021-22. The Repository has a history of making corrections and improvements to data and metadata based on such feedback including taking down content that was felt to impinge on the rights of 3rd parties. In addition, metadata and subject experts in the Repository have an active role to update, enhance and republish the metadata for Content Groups provided to Web Users.

SUPPORTING EVIDENCE:

R11.1) Digital Preservation Data Integrity Policy:

<https://doi.org/10.34812/173d-f765>

R11.2) Data Foundry:

<https://data.nls.uk>

Reviewer Entry

Reviewer 1

Comments:

accept

Reviewer 2

Comments:

accept

12. Workflows

R12. Archiving takes place according to defined workflows from ingest to dissemination.

Compliance Level:

4 – The guideline has been fully implemented in the repository

Reviewer Entry

Reviewer 1

Comments:

4 – The guideline has been fully implemented in the repository

accept

Reviewer 2

Comments:

4 – The guideline has been fully implemented in the repository

accept

Response:

The Repository's Digital Preservation team documents and compiles workflows for data in the OAIS Archive into a single Digital Preservation and Access Workflows document [R12.1]. The following points complement the information in that document:

WORKFLOWS

- Data quality criteria and checks are referred to as "Submission QA" in the Digital Preservation and Access Workflows document and are documented in more detail in the Digital Preservation Content Register that records the assessment of content before it is ingested into the OAIS Archive and the Digital Preservation and Access Plan [R12.2].

- The Repository aims to standardise ingest and management of data as much as possible but recognises that differences exist that require tailored "recipes" with bespoke processing and qualitative and quantitative data checks. Tailored ingest recipes exist for the following Content Groups:

- 1) Library Digitised Still Image (non-map).
- 2) Digitised Maps.
- 3) Moving Image web video packs.
- 4) Moving Image Preservation Masters.
- 5) Unlocking Our Sound Heritage.
- 6) Scottish government publications (non-legal deposit)
- 7) All others.

- Once ingested the data is subject to the same long-term management – 3 distinct copies are made, and fixity checks are undertaken in line with the Digital Preservation Data Integrity Policy [R12.3].

- A similar diversity of workflows is in place to disseminate data in the OAIS Archive to the Repository's web services:

- 1) Moving Image.
- 2) Digital Gallery (including IIIF).
- 3) Data Foundry.
- 4) Maps.

- Staff with permission from the Content Group Controller can also download data from the Repository's OAIS Archive via download tools.

HANDLING OF DATA

- The Repository's Collection Development Policy explains to suppliers of potential material (external producers) how the

material will be used [R12.4].

- The Repository provides information to the Web Users designated community about how it can re-use data provided to them [R12.5].

- Content Group Controllers (data producers) are informed of the steps taken by the Repository's OAIS Archive to preserve access to data while agreeing a Digital Preservation and Access Plan with OAIS Archive staff. This includes a description of how the users (Content Group Controllers, staff identified by the Content Group Controllers, and Web Users) will be provided with access.

CHANGE MANAGEMENT AND DECISIONS

- Changes to workflows and processes happen regularly, largely in the pursuit of improvements. Such changes are controlled by OAIS Archive staff if the outcomes do not contradict policy or Digital Preservation and Access Plans.

- Significant changes to workflows that impact the Repository's OAIS Archive, its data, web services that use the data, existing policy, or Digital Preservation and Access Plans are evaluated by the Digital Preservation Steering Group in consultation with relevant Content Group Controllers. Final decisions are made by the Digital Preservation Steering Group or escalated to the Library Leadership Team.

SUPPORTING EVIDENCE:

R12.1) Digital Preservation and Access Workflows:

<https://doi.org/10.34812/eamg-jq88>

R12.2) Example records in the Digital Preservation Content Register:

<https://doi.org/10.34812/8b0t-e697>

R12.3) Digital Preservation Data Integrity Policy:

<https://doi.org/10.34812/173d-f765>

R12.4) Collection Development Policy:

<https://doi.org/10.34812/gpde-cw03>

R12.5) Re-using material:

<https://www.nls.uk/using-the-library/copying-services/permission>

Reviewer Entry

Reviewer 1

Comments:
accept

Reviewer 2

Comments:
accept

13. Data discovery and identification

R13. The repository enables users to discover the data and refer to them in a persistent way through proper citation.

Compliance Level:

3 – The repository is in the implementation phase

Reviewer Entry

Reviewer 1

Comments:
3 – The repository is in the implementation phase
accept

Reviewer 2

Comments:
3 – The repository is in the implementation phase
accept

Response:

Data discovery and identification is provided to the Repository's Content Group Controller and Web User designated communities.

CONTENT GROUP CONTROLLERS

Every Content Group in the Repository is paired with a Content Group Controller who is responsible for it. Search, resolution, citation, and use are provided in the following ways:

1) An ingest receipt is provided to the Content Group Controller or their representative by OAIS Archive staff after an ingest request is fulfilled. The receipt includes a list of the OAIS Archive file paths and persistent identifiers that relate to them. The persistent identifiers use an internal scheme, minter and resolver that are managed by the Repository and are referred to as NLS DOD (National Library of Scotland Digital Object Database) persistent identifiers. This information can be used by the Content Group Controller to search and retrieve files from the OAIS Archive based on filename, path, or

persistent identifier through scripts, download tools, and through a search and browse web interface for Repository staff. Furthermore, each Content Group is allocated an overarching persistent ID and descriptive record in the Digital Preservation Database which is recorded in the Digital Preservation Content Register.

2) Some Content Groups have additional descriptive hierarchies to provide more context to the data and allow searching within the Digital Preservation Database by titles, descriptions, and indexing terms. Descriptive metadata is particularly rich for the "Library Digitised Still Image" Content Group. Searching is done either directly against the metadata in the database, through a web interface for Repository staff, or an equivalent but older Microsoft Access interface that also allows for metadata creation and editing. The latter two approaches present the complicated database table structure in more user-friendly ways to allow the staff to undertake routine searches and tasks easily.

The relationship between agents, events, objects, and rights are managed in a way that complies with the PREMIS data dictionary. The rich descriptive metadata of digitised Content Groups allows them to be exported from the OAIS Archive and/or collecting databases to comply with several standards including MARC, MODS, Dublin Core and IIIF. It is worth noting that the Repository is a signatory to the Europeana Data Exchange Agreement [R13.1], and the Jisc Discovery Open Metadata Principles [R13.2].

WEB USERS

The Repository offers several web services that allow the Web Users designated community to search a subset of data in the Repository's OAIS Archive. The web services use copies and/or additional derivatives of the data that are suitable for browsers. The OAIS Archive runs metadata export routines using the Digital Preservation Database and Collection databases to create standardised metadata to power the web services. Each offers its own interface suited to the content it provides access to. For example, the maps interface has a geographic Google maps search layer. All of the web services support web crawling and harvesting for direct access from search engines. Additional details for primary services are summarised below:

DIGITAL GALLERY

- URL: <https://digital.nls.uk/gallery/>
- Metadata standards: IIIF, tags use LCNAF, TGN, AAT, LCSH, and TGM as sources of controlled vocabulary
- Form of data citations: Permalink and shareable links using NLS DOD persistent identifiers
- Machine harvestable?: IIIF volumes are harvestable via a top-level collections-based json file that provides access to all IIIF manifests (<https://view.nls.uk/collections/top.json>)

DATA FOUNDRY

- URL: <http://data.nls.uk/>
- Metadata standards: <https://data.nls.uk/about/standards/>
- Form of data citations: Suggested citations using DOI persistent identifiers
- Machine harvestable?: Datasets available for download

MOVING IMAGE

- URL: <https://movingimage.nls.uk/>
- Metadata standards: FIAF cataloguing standards, tags use LCGFT
- Form of data citations: Shareable links using system identifiers that have the potential to be turned into persistent identifiers. They will be considered as part of the Repository's persistent identifier framework, due for completion in 2021-22.
- Machine harvestable?: No

MAPS

- URL: <https://maps.nls.uk/>
- Metadata standards: ISBD, tags use LCNAF
- Form of data citations: Shareable links using NLS DOD persistent identifiers
- Machine harvestable?: Recent additions have an RSS feed: <https://maps.nls.uk/feed.xml>

Some Repository content is available and searchable in secondary web services, such as the Repository's own aggregated search service called Library Search, and those not managed by the Repository, such as Europeana and Internet Archive, that use additional standards.

SUPPORTING EVIDENCE:

R13.1) Europeana Data Exchange Agreement

<https://pro.europeana.eu/page/the-data-exchange-agreement>

R13.2) Jisc Discovery Open Metadata Principles

<http://discovery.ac.uk/businesscase/principles/>

Reviewer Entry

Reviewer 1

Comments:

accept

Reviewer 2

Comments:

accept

14. Data reuse

R14. The repository enables reuse of the data over time, ensuring that appropriate metadata are available to support the understanding and use of the data.

Compliance Level:

3 – The repository is in the implementation phase

Reviewer Entry

Reviewer 1

Comments:

3 – The repository is in the implementation phase

accept

Reviewer 2

Comments:

3 – The repository is in the implementation phase

accept

Response:

The Repository blends its data and metadata in a way that supports agreed commitments to understandability and use needs of its designated communities. The Repository is continuing to improve its understanding of the formats in its care to increase access to new communities.

METADATA

The Repository's OAIS Archive staff work with the Content Group Controller to agree a Digital Preservation and Access Plan prior to ingest. The plans are stored in the Digital Preservation Content Register and record what data and metadata are required to support use and understandability of the content for specific designated communities, for specific preservation periods [R14.1]. Broadly speaking the communities include the Content Group Controller and members of Repository staff they identify and, for some content, Web Users. Any partial Digital Preservation and Access Plans that exist will be upgraded to full plans in 2021-22.

Metadata provided to the Web User designated community is rich, using metadata from the Digital Preservation Database that is often merged with metadata from Collection databases. This metadata is typically descriptive and structural to allow the content to be searched and used to represent the physical collections from which they frequently derive. Web services are also adapted over time to meet the needs of Web Users e.g., to support wider mobile device use. Finally, the Library is committed to making web services accessible [R14.2].

Metadata for the Content Group Controller designated community includes descriptive and structural metadata as well as rights, technical, administrative, and preservation metadata. However, Content Groups that are exclusively for Repository staff tend to have very limited descriptive metadata. Understandability is provided by returning the data as deposited with filenames, file structure and file contents intact. In addition, the Repository's OAIS Archive will have requested supporting documents, for example a descriptive overview of the content, for ingest to achieve the level of understandability described in the Digital Preservation and Access Plan.

FORMATS

Broadly speaking, the Repository has control over the formats used in its digitisation programme and creates a range of derivatives and formats for the Web User designated community. Over time the Repository enhances its offering to the community to meet their evolving needs. Recent additions include using the ALTO XML standard for OCR text documents, and the provision of IIIF compatible content.

For Content Groups where the Repository has less control over formats, DROID and PRONOM are used to identify file formats and help determine what software may be needed to make the content accessible and understandable. This work is ongoing, and a long-term goal of the Repository is to build a Software and License Library to promote reuse through emulation.

The Repository may change formats over time or create additional ones. Changes to formats will be overseen by the

Digital Preservation Steering Group working with affected Content Group Controllers. Changes are not permitted where a Content Group needs to demonstrate authenticity and the Repository cannot reverse the changes.

Through its membership of the wider digital preservation community (e.g. as an active member of the Legal Deposit Libraries [R14.3], the UK Web Archive [R14.4], the International Internet Preservation Consortium [R14.5], and the Digital Preservation Coalition [R14.6]) the Repository researches new formats as well as techniques to allow existing formats to be reused.

REVIEW

Starting in 2021-22 OAIS Archive staff will conduct a biennial review of the Digital Preservation and Access Plans with the Content Group Controllers. The review will determine if any changes are required to continue to meet the preservation, access and understandability commitments made in the plan to the designated communities.

SUPPORTING EVIDENCE:

R14.1) Example records in the Digital Preservation Content Register:

<https://doi.org/10.34812/8b0t-e697>

R14.2) Website accessibility statement:

<https://www.nls.uk/about-us/website-accessibility-statement>

R14.3) Agency for the Legal Deposit Libraries

<https://www.legaldeposit.org.uk/>

R14.4) UK Web Archive

<https://www.webarchive.org.uk/en/ukwa/info/about>

R14.5) International Internet Preservation Consortium (membership details)

<https://netpreserve.org/about-us/members/national-library-scotland/>

R14.6) Digital Preservation Coalition list of members

<https://www.dpconline.org/about/members>

Reviewer Entry

Reviewer 1

Comments:

accept

Reviewer 2

Comments:
accept

TECHNOLOGY

15. Technical infrastructure

R15. The repository functions on well-supported operating systems and other core infrastructural software and is using hardware and software technologies appropriate to the services it provides to its Designated Community.

Compliance Level:

4 – The guideline has been fully implemented in the repository

Reviewer Entry

Reviewer 1

Comments:
4 – The guideline has been fully implemented in the repository
accept

Reviewer 2

Comments:
4 – The guideline has been fully implemented in the repository
accept

Response:

INFRASTRUCTURE DEVELOPMENT

The Repository has an infrastructure strategy that is based on replacing legacy systems and conforming to new and emerging security standards while focusing on the drive to digital. The Repository continues to implement its cloud-first approach for infrastructure and will review all available options to determine if cloud or on-premises solutions are most fit for purpose. In 2020 and 2021 the Repository is undertaking a review of its Digital Asset Management Systems which includes components in the OAIS Archive. The review, and significant changes to the OAIS Archive will involve the Digital Preservation Steering Group that govern it.

SOFTWARE

The Repository's IT team maintains a hardware and software asset directory following ITIL standard recommendations for e.g., a Definitive Media Library [15.1], and uses management software to identify operating systems and other software on Repository devices. This helps to ensure that Repository infrastructure, software applications, and operating systems are kept up-to-date, and maintain the functionality required to deliver data held in the OAIS Archive.

Operating system and application patching is managed and monitored under an automated system ensuring cyber compliance.

Software licenses are recorded in an internally developed database and maintained by the Repository's IT team. Installations are also recorded ensuring license compliance.

OAIS Archive staff manage a Preservation Software Register that records the software used to process and manage data in the OAIS Archive [R15.2]. The software is a mix of commercial and community software and includes Foxit PDF compressor, Kakadu, Microsoft SQL Server, Scality, AWS CLI, CloudBerry, FFmpeg, MediaInfo, Jpylyzer, Exif Tool, ImageMagick, DROID and solr. Work between 2021 and 2023 will identify and manage rendering software.

CAPACITY AND CAPABILITY

Around 1 PB of storage is available to the Repository's OAIS Archive in triplicate and this has grown over the last 20 years to meet the growth in data. A suitably sized and performing Microsoft SQL Server database is provided to support the Digital Preservation Database. Virtual Machine farms are available in Edinburgh and Glasgow with multiple 10GB network connections to local storage to facilitate ingest, access, and management. The Repository provides its Web Users designated community with access to web services through a single 1GB internet connection through Janet provided by Jisc. The Repository is working with Jisc to implement a secondary internet circuit into a secondary facility with divergent links providing resilience in the event of a failure. In addition, more services are provided via the cloud both internally to the Repository, and externally to its Web Users. Utilisation of the internet circuit is being monitored to ensure the circuit connection grows with the Repository's requirements.

The Repository has access to a dedicated IT team providing Helpdesk, networking, database, storage, and other infrastructure support. It can also use an internal team of developers to automate workflows and create new tools and systems.

DISASTER RECOVERY AND BUSINESS CONTINUITY

The Repository uses its Business Continuity Framework and Procedures to manage disaster recovery and business continuity [R15.3]. This supports the OAIS Archive and the services it provides to its designated communities. In 2022-23

the Repository will develop and deploy additional test plans for key components of its OAIS Archive that are not yet tested and simulate their failure and recovery.

Most of the Repository's systems are virtualised and are configured to replicate to a secondary site in the event of a failure. The Repository's IT teams use a hardware based alert system to receive notifications when servers used by the OAIS Archive have failed or are predicted to fail. The two independent preservation storage clusters in Edinburgh and Glasgow are configured using erasure coding [R15.4] instead of RAID as it reduces the overhead and time to reconstruct data in the event of a failure, and the diversification and distribution of risk across all 3 storage locations also assists in disaster recovery.

SUPPORTING EVIDENCE:

R15.1) ITIL recommended practice:

<https://en.wikipedia.org/wiki/ITIL>

R15.2) Software Preservation Register:

<https://doi.org/10.34812/90y2-ez11>

R15.3) Business Continuity Framework and Procedures:

<https://doi.org/10.34812/as10-8m98>

R15.4) What is erasure coding?

<https://stonefly.com/blog/understanding-erasure-coding>

Reviewer Entry

Reviewer 1

Comments:

accept

Reviewer 2

Comments:

accept

16. Security

R16. The technical infrastructure of the repository provides for protection of the facility and its data, products, services, and users.

Compliance Level:

4 – The guideline has been fully implemented in the repository

Reviewer Entry

Reviewer 1

Comments:

4 – The guideline has been fully implemented in the repository accept

Reviewer 2

Comments:

4 – The guideline has been fully implemented in the repository accept

Response:

RISK MANAGEMENT

The Repository uses a Risk Management Framework with standardised risk registers to record the assessment of risks that could affect the Repository, acceptable levels of risk, and the mitigation actions to reduce them [R16.1]. Of note are the Corporate Risk Register and the Digital Preservation Risk Register managed by the Library Leadership Team and the Digital Preservation Steering Group respectively. Some of the risks are identified through interviews with Content Group Controllers and an analysis of their data by OAIS Archive Staff. Risks associated with specific Content Groups are also recorded in the Digital Preservation Content Register [R16.2].

SECURITY AND AUTHENTICATION

The Repository manages security as described by the Information Security Policy [R16.3] and the Access Control Procedure [R16.4]. They cover physical and digital data security and encompass those physical and digital components used by the OAIS Archive. All Repository staff agree to the Acceptable Use Policy which, for example, restricts the installation of software on devices [R16.5]. The Repository has previously achieved UK Cyber Essentials certification [R16.6] and is working towards re-certification in 2022-23.

The following authentication and authorisation procedures are used for the various components of the OAIS Archive in addition to those mentioned in IT security policies:

library devices used at ingest and pre-ingest: Managed by the IT team using Windows Active Directory. OAIS Archive staff responsible for ingest do not have delete permissions for the content passed to them by the Content Group Controller or their representative (as internal data producers).

Digital Preservation Database (Microsoft SQL Server): Managed by the IT team at the software, server and database level. Authentication uses Windows Active Directory. Role-based table level security and architecture managed by

database managers.

Storage (2 local copies): Managed by the Digital Preservation team and IT team through S3 authentication. No delete permissions. Versioning used to avoid destructive overwrites. Changes to security or policies require simultaneous involvement of the Digital Preservation team and the IT Team.

Storage (3rd remote copy): Managed by the Digital Preservation team through S3 authentication. No delete permissions. Versioning used to avoid destructive overwrites. Multi-Factor Authentication required to change security or policies. Jisc provide additional security for the Repository's internet connections including DDoS mitigation.

Library devices used to access OAIS Archive data by the Digital Preservation team and the Content Group Controllers designated community: Managed by the Digital Preservation team and IT team through Windows Active Directory and S3 authentication. Repository staff outside of those teams only have read access to one of the 3 copies and only for the Content Groups in S3 buckets they have credentials for.

Web services used to provide content to the Web Users designated community: Managed by the Systems and Applications Development team. User web applications protected by routinely escaping and/or sanitising form and URL variable input from XSS attacks [R16.7], SQL injection [R16.8], and LDAP injection [R16.9]. Users are authenticated as required via SAML 2.0 and/or OAuth sessions while ensuring user passwords are salted with one-way encryption using cryptographic hashes. Only copies and web suitable derivatives stored outside of preservation storage are delivered to Web Users. Jisc provide additional security for the Repository's internet connections including DDoS mitigation.

SUPPORTING EVIDENCE:

R16.1) Risk Management Framework:

<https://doi.org/10.34812/8kcb-vz59>

R16.2) Example records in the Digital Preservation Content Register:

<https://doi.org/10.34812/8b0t-e697>

R16.3) Information security policy:

<https://doi.org/10.34812/yhye-x905>

R16.4) Access Control Procedure:

<https://doi.org/10.34812/dq3z-z559>

R16.5) Acceptable Use Policy:

<https://doi.org/10.34812/jgg0-en54>

R16.6) UK Cyber Essentials overview:

<https://www.ncsc.gov.uk/cyberessentials/overview>

R16.7) Wikipedia page describing XSS and XSS attacks

https://en.wikipedia.org/wiki/Cross-site_scripting

R16.8) SQL injection

https://en.wikipedia.org/wiki/SQL_injection

R16.9) LDAP injection

https://en.wikipedia.org/wiki/LDAP_injection

Reviewer Entry

Reviewer 1

Comments:

accept

Reviewer 2

Comments:

accept

APPLICANT FEEDBACK

Comments/feedback

These Requirements are not seen as final, and we value your input to improve the CoreTrustSeal certification procedure. Any comments on the quality of the Requirements, their relevance to your organization, or any other contribution, will be considered as part of future iterations.

Response:

Reviewer Entry

Reviewer 1

Comments:

I do not have any other issues or comments for this application, I believe the applicant has done a great job. I would advise the approval of the application.

Reviewer 2

Comments:

This is a very well-done self-assessment that points to future developments. I would suggest accepting it.