Archives West Midlands

Digital Preservation Policy template

E: archiveswestmidlands@gmail.com

www.archiveswestmidlands.wordpress.com

Policy Owner(s)	Archives West Midlands Board of Trustees
Version	1.1
Prepared by	Charlene Taylor
Approved by	
Date approved	
Review date	31st October 2020

Contents

Acknowledgements

1. Introduction

[Insert service name] is a subscribed member of [Archives West Midlands](#) (AWM). AWM is a strategic partnership of and for archive services in the West Midlands region, which seeks to maximise the benefits of working together and to realise funding opportunities.

AWM is committed to seeking ways to develop a regional solution for digital preservation. It recognises that by working together its member services are in a stronger position to make progress. By seeking funding opportunities and pooling existing knowledge and resources, Archives West Midlands seeks to take significant steps towards helping to secure the digital heritage of the West Midlands. By working collaboratively as a region, AWM aims to:

- Share knowledge and skills amongst services for the benefit of all members.
- Deliver greater efficiencies and savings by working together so member services can continue to meet their objectives, even with reduced resources.
- Maximise the expertise of staff in the region to ensure services get the best return on investment.
- Save time and resources by sharing information and creating joint standards, guidelines and templates to use internally and to disseminate to depositors.
- Work together to increase chances of attracting external funding and sponsorship.

As part of its commitment to advancing digital preservation activities in the West Midlands, AWM successfully obtained funding from The National Archives' Sustainability Fund to enable the preparation of this Digital Preservation Policy. The funding received also enabled the preparation of an Archives West Midlands' report on Accessioning Born-digital material.

As a member of Archives West Midlands, **[Insert service name]** has adopted this jointly prepared policy statement, with modifications made where appropriate to address internal governance.

2. Principle Statement

Digital Preservation looks specifically at the activities necessary to preserve, and to ensure continued long-term access to, digital material. When referring to digital materials, we include:

- Digitised non-digital collections
- Born digital resources, which have been created and managed electronically. This includes information created as part of the day-to-day business of an organisation

[Insert mission statement of service, for example, " We protect, preserve, manage, record, interpret, share and promote the history and historic environment of…."]. Our commitment to secure our documentary heritage remains the same regardless of the format in which records are received. The purpose of this policy is to state and communicate the principles that guide **[Insert service name]**'s activities to preserve our digital information resources. Further

documents, procedures and guidance will be developed in the future to address specific aspects around the implementation of this policy.

Digital materials pose extra challenges to repositories in terms of maintaining long-term access. Unlike paper-based records, digital material has only a short timeframe in which action can be taken to secure its accessibility. The volume, complexity and importance of data that is being produced digitally is growing on a huge scale and it is therefore imperative to act now to establish procedures for effectively dealing with digital material.

Although digital technology provides considerable opportunity for rapid and efficient access to information, there is a very real threat that digital materials are created in such a way that even short-term viability cannot be assured, therefore there is much less prospect of access by future generations. Threats of technological obsolescence and rapid physical deterioration of digital material means that there is a need for a very different approach to be taken in its management – one which is proactive and which is planned and reviewed at regular intervals.

There are a number of pressing reasons for action to be taken:

* Digital material will quickly become inaccessible. Loss of data will need to be justified to depositors and to other stakeholders with an interest in or need for access to the material.
* **[Insert service name]** has statutory obligations to provide access to Public Records. Our obligations will remain the same regardless of the format Public Records are received in. **[This point is optional and may be removed if you are not a P.O.D.]**
* If access to digital surrogates cannot be maintained beyond the short-term then it may be difficult to justify the initial, often substantial, investment in creating digital resources.
* Retrospective preservation of digital material can be prohibitively costly or, in a worst case scenario, impossible due to media deterioration. It is widely acknowledged that the most cost-effective means of ensuring continued access is to consider preservation implications as early as possible, preferably at the creation stage.
* Digital material has value. This may be in terms of the value of reproducing the material, or in terms of the value of its content for informational, democratic, identification, well-being and evidential purposes, especially where legal and regulatory compliance is implied.

3. OAIS (Open Archival Information System) reference model

When embarking on digital preservation work it is useful to gain a basic grasp of the OAIS (Open Archival Information System) model. The model provides a shared vocabulary that can be used by information professionals and IT staff to communicate when working on digital preservation projects and is adopted by digital preservation systems such as Preservica. A brief introduction is available in the Digital Preservation Handbook[1] and the Paradigm Workbook[2]. A more detailed

---

[1] Standards and Best Practice, Digital Preservation Handbook https://www.dpconline.org/handbook/institutional-strategies/standards-and-best-practice, Date accessed 19/11/2018.
[2] *Introduction to OAIS*, Paradigm, http://www.paradigm.ac.uk/workbook/introduction/oais.html, Date accessed 19/11/2018.

introduction is given in a Technology Watch Report produced by the Digital Preservation Coalition.[3]

4. Scope of the Policy

This digital preservation policy applies to all digital collection material *held for the purpose of long term preservation* by **[Insert service name]**.This policy also applies to any preservation metadata and persistent identifiers associated with such digital collections

The information resources in digital form covered by this policy can be categorised as follows:
- Born digital resources, which have been created and managed electronically
- Made digital resources, which were originally created in non-digital form and have subsequently been converted to digital form for business, preservation or access purposes

To ensure that records are submitted in a suitable condition for acceptance into the archive, the following principles apply to the digital resources that will be collected and preserved under the terms of this policy:
- Appraisal and selection procedures for digital material must comply with **[Insert name and link to your service Acquisitions/ Collections Development Policy as appropriate]**.
- Digital material must be presented in file formats that are accepted and can be appropriately managed by the service, as detailed in **[insert name a link to list of preferred file formats your service can manage]** Material offered in non-preferred formats will be assessed on a case-by-case basis by archive staff and advice will be given where any deposits cannot be accepted.
- Minimum levels of descriptive and technical metadata must be supplied at the point of deposit **[as detailed in our digital records deposit form, link to if available]** to ensure the efficient and appropriate long-term preservation of the material

[If appropriate your service may wish to list the individuals, institutions and organisations from whom records will be collected, such as County Council, University governing body and departments, Police, NHS or other public bodies, businesses, private depositors – incl. families, people who may have inherited the records and aren't in a position to appraise/apply metadata. Those services identified as a Place of Deposit under the Public Records Act will also have additional obligations and may wish to include a statement relating to this. This section is entirely optional and depends upon the requirements of your service and how specific you wish your policy to be.]

---

[3] Brian Lavoie, *The Open Archival Information System (OAIS) Reference Model: Introductory Guide (2nd Edition)*, DPC Technology Watch Report 14, 02 October 2014, https://www.dpconline.org/docs/technology-watch-reports/1359-dpctw14-02/file. Date accessed 19/11/2018.

5. Preservation Objectives

[Each service will have a different, practical approach to how they preserve their digital material. The preservation actions they carry out will depend entirely upon where they currently find themselves in their digital preservation journey, along with the systems and procedures adopted by that service. The following objectives are optional for inclusion in your policy. Please delete/add to as appropriate for your current levels of digital preservation activity].

[Insert service name] is committed to preserving the archival version: the fullest, highest-quality available version of a digital resource, whenever possible; and the descriptive, structural, and administrative metadata associated with it. To enable the service to achieve this objective, **[Insert service name]**:

- Will seek to preserve the original bytestream of digital objects
- Will actively monitor collections for corruption and unauthorised changes
- Will continue to investigate and test the suitability of both open source and widely implemented proprietary software with excellent export formats, in order to procure the digital preservation system best suited to the service.
- Will continue to document, monitor and refresh its technical processes over time
- Will create and manage its digital collections in accordance with standards which are commonly adopted within the heritage sector and digital preservation community
- May undertake preservation activities, such as migration from one file format to another file format, to ensure that digital collections are accessible in current computing environments
- Will ensure that any preservation activities performed on digital collections are tested, evidenced-based, and recorded
- Will ensure that staff are provided with appropriate training around digital preservation activities to ensure they can fulfil the requirements of their job roles
- Will conduct regular risk assessments, auditing and feedback gathering to ensure any processes and systems adopted continue to be the most appropriate for the service
- Will seek to ensure management of its digital collections adheres to the same legislation that applies to all collections under its care, including **[delete/add as appropriate for your service]**:
  - Freedom of Information Act
  - Data Protection Act
  - Copyright Act.

- Will seek sufficient resources and support to ensure that its digital preservation activities are viable and sustainable for the long-term

6. Context

This policy is designed to be read and to operate in conjunction with the following existing policies and documentation **[link to/delete/add as appropriate for your service]**:
- Collections Management Policy

- Collections Information Policy
- Acquisitions/Collections Development Policy
- Collections Development Plan
- Access Policy
- Conservation and Preservation Policy
- Collections Care and Conservation Plan
- Digital Preservation Strategy
- Digitisation Policy
- Records Management Policy
- Information Security Policy

7. Roles and Responsibilities

Responsibility for the preservation of digital material lies primarily with **[Insert service name]** staff, who develop and manage the collections, have responsibility for service policies and are the primary point of contact for the creators and users of digital materials. The implementation of this digital preservation policy will require working across teams within **[insert name of parent organisation, e.g. County Council/University]** and, on occasion, external partners. The following can therefore be considered stakeholders in this policy:

- **[Insert name of parent organisation]** as record creators and all other contributing depositors, some of whom have statutory obligations. Record creators will be responsible for ensuring that digital resources are created and managed in accordance with this and other associated policies.
- The records creators and **[insert name of Archive/Collections]** team who are responsible for the creation and management of metadata associated with digital records.
- The **[insert name of Archive/Collections]** team who ensure that archival material is preserved and made available.
- The **[insert name of Senior Management team of service]** who must demonstrate that the organisation is fit for purpose in every respect, including the managing and preserving of its digital collections, archival or otherwise.
- **[Insert name of parent organisation]** who require authentic and accurate information to be preserved and made available for open and democratic decision-making.
- Record users, who rely on correct and authentic information being kept and made available, and whose needs help determine what is important for preservation.
- Staff in associated departments within **[Insert name of parent organisation]**, with whom the service must collaborate to ensure the efficient implementation of this policy, including **[insert names of relevant teams, e.g. IT department, Records/Information Management department, Directorate etc.]**
- [**Include/delete as appropriate**] The National Archives who regulate our statutory duties under the Public Records Act.
- Other potential users.

Implementation of the policy:

- The **[insert role title of the senior officer responsible for oversight of collections management at your services, i.e. Collections Manager/Head of Service]** is responsible for the implementation and communication of this digital preservation policy, and for updating the strategy for implementation as required.
- The **[insert name of team or role title of individual who will action this policy on a day-to-day basis, i.e. Archive team/ Collections team]** is responsible for overseeing the day-to-day implementation of this digital preservation policy.

8. Archives West Midlands policy statement

Archives West Midlands is committed to advancing the implementation of practical digital preservation activities amongst its member services. Together, it will continue to collaborate with member services and to seek funding opportunities that will enable this area of work to develop further.

AWM's primary commitment is to help member services to achieve Level One of the National Digital Stewardship Alliance's (NDSA) Levels of Digital Preservation. The Archive Service Accreditation Standard now requires that services self-evaluate their levels of digital preservation activity using the NDSA Levels as a guide, and AWM believes that achieving Level One of this standard would be a key milestone in achieving the required level of digital preservation capability. Please see **Appendix A** for the full NDSA Levels table, which shows the requirements for each level.

AWM will continue to seek ways to resource a digital preservation system for use by member services, which will include the investigation and trial of both proprietary and open-source systems that may suit the needs of individual services.

AWM acknowledges that a cross-region solution may not be feasible for all elements of digital preservation activity within the West Midlands. AWM will continually monitor and assess the needs of its members, alongside the progress of digital preservation research further afield, and will always seek to act in the best interests of its member services.

9. Implementation and Strategy

[Insert service name] may implement different preservation strategies over time, and for different types of digital resource. These strategies will be selected according to the requirements of particular resources, current best practice, and an assessment of the resources required for implementation.

In order to make progress to achieve the minimum required NDSA Level One standard, **[Insert service name]** will continue to work with Archives West Midlands to investigate a regional approach to digital preservation activities. The next steps in implementing this policy are:

- To perform an audit of all collections, which will identify all digital material currently held by the service.
- Creation of a Digital Asset Register, which will systematically record all digital content held by the service. Information about file formats and software used, along with where and how data is stored, will help the service to assess risk. Assessing risk can help to highlight any specific threats to the continuity of digital resources.
- To continue the region-wide investigation of both proprietary and open-source digital preservation systems. This will allow an assessment to establish which system suits the needs of the service in practical terms and is financially viable for the long-term
- To adopt a continuous process of risk assessment with regards to our digital collections, to ensure [insert service name] is offering a proactive approach towards securing our digital heritage.

10. Review date

This Policy will be reviewed at least every two years, or as required to take account of changing circumstances.

Appendix A – NDSA Levels of Preservation[4]

	Level One (Protect Your Data)	Level Two (Know Your data)	Level Three (Monitor Your Data)	Level Four (Repair Your Data)
Storage and Geographic Location	Two complete copies that are not co-located For data on heterogeneous media (optical disks, hard drives, etc.) get the content off the medium and into your storage system	At least three complete copies At least one copy in a different geographic location/ Document your storage system(s) and storage media and what you need to use them	At least one copy in a geographic location with a different disaster threat Obsolescence monitoring process for your storage system(s) and media	At least 3 copies in geographic locations with different disaster threats Have a comprehensive plan in place that will keep files and metadata on currently accessible media or systems
File Fixity and Data Integrity	Check file fixity on ingest if it has been provided with the content Create fixity info if it wasn't provided with the content	Check fixity on all ingests Use write-blockers when working with original media Virus-check high risk content	Check fixity of content at fixed intervals Maintain logs of fixity info; supply audit on demand Ability to detect corrupt data Virus-check all content	Check fixity of all content in response to specific events or activities Ability to replace/repair corrupted data Ensure no one person has write access to all copies
Information Security	Identify who has read, write, move, and delete authorization to individual files Restrict who has those authorizations to individual files	Document access restrictions for content	Maintain logs of who performed what actions on files, including deletions and preservation actions	Perform audit of logs
Metadata	Inventory of content and its storage location Ensure backup and non-collocation of inventory	Store administrative metadata Store transformative metadata and log events	Store standard technical and descriptive metadata	Store standard preservation metadata

---

[4] National Digital Stewardship Alliance, Levels of Preservation: http://ndsa.org/activities/levels-of-digital-preservation/

File Formats	When you can give input into the creation of digital files encourage use of a limited set of known open file formats and codecs	Inventory of file formats in use	Monitor file format obsolescence issues	Perform format migrations, emulation and similar activities as needed
Access	Determine designated community[1] Ability to ensure the security of the material while it is being accessed. This may include physical security measures (e.g. someone staffing a reading room) and/or electronic measures (e.g. a locked-down viewing station, restrictions on downloading material, restricting access by IP address, etc.) Ability to identify and redact personally identifiable information (PII) and other sensitive material	Have publicly available catalogues, finding aids, inventories, or collection descriptions available to so that researchers can discover material Create Submission Information Packages (SIPs) and Archival Information Packages (AIPs) upon ingest[2]	Ability to generate Dissemination Information Packages (DIPs) on ingest[3] Store Representation Information and Preservation Description Information[4] Have a publicly available access policy	Ability to provide access to obsolete media via its native environment and/or emulation