1. Executive Summary

Local authorities are responsible for managing and archiving their own records, including digital records.

Most official business within local authorities is done using electronic systems and produces digital records. The switch from paper to digital has happened in most local authorities gradually over a period of up to twenty years, and it is likely that there are many systems, including legacy systems, holding digital records within each authority.

While current digital records may be kept safe in active systems, there is a legislative requirement under the Public Records (Scotland) Act 2011[1] for authorities to identify all records that have enduring value and which require to be permanently preserved, some of which may be stored in legacy systems. These records must be identified under an authority's retention schedule, managed securely as current and semi-current business records and securely transferred to appropriate archival storage. These digital records then form part of the permanent archive of the authority.

Other legislation requiring public bodies to properly manage their public records includes the Data Protection Act 1998,[2] the Freedom of Information (Scotland) Act 2002[3] and the Environmental Information (Scotland) Regulations 2004.[4]

The point at which these digital records should be transferred to the archive, often 10, 15 or 20 years after creation, is in many cases now overdue. There is a need to

[1] Public Records (Scotland) Act 2011 http://www.legislation.gov.uk/asp/2011/12/contents

[2] Data Protection Act (1998) http://www.legislation.gov.uk/ukpga/1998/29/contents

[3] Freedom of Information (Scotland) Act 2002 http://www.legislation.gov.uk/asp/2002/13/contents

[4] Environmental Information (Scotland) Regulations 2004 http://www.legislation.gov.uk/ssi/2004/520/contents/made

safeguard these records permanently, but the systems required to manage this are often not in place. There is a vicious circle at work here: most local authority archives do not have appropriate storage for digital records because as yet they have not had digital records to manage. However, archives are not given digital records to manage because they have no storage.

Dedicated storage for the permanent preservation of digital records is a necessary part of ensuring the records are secured. The form that this storage takes is not prescribed; there are many ways of acquiring storage, as detailed later in this guidance, including the re-purposing existing resources within the authority, cloud services, and acquisition of new hardware. The NRS case study will demonstrate a practical solution to this problem.

Once records are secured, the rest of the digital preservation process can follow. This will include analysing and managing the data and ultimately making the records accessible to the public. These final stages can be planned in detail at a later date: the priority must be to securely store the records so that the records are safe.

2. Introduction

2.1 Digital Preservation for local authorities

National Records of Scotland (NRS) has produced this guidance to digital preservation to assist local authorities to meet their obligations to permanently preserve archives and maintain digital records of long term value.

All named public authorities are required to manage records in line with their obligations under the Public Records (Scotland) Act 2011 (the Act). Under the Act, each Scottish local authority must submit a Record Management Plan (RMP)[5] for the Keeper of the

[5] Public Records (Scotland) Act 2011 s 1
(2)An authority's records management plan must—

Records of Scotland's (the Keeper) agreement. In this way, the Act aims to safeguard public records created and held within the authorities. The Act requires public authorities to have 'Proper Arrangements' in place for the management of their public records. These include the transfer to an archive of records selected for permanent preservation. Further details about the requirement are given in the Supplementary Guidance on Proper Arrangements for the Archiving of Public Records[6] issued by NRS.

The authority's policies and procedures governing the management of its public records, including digital records, are scrutinised by the Keeper's assessment team when assessing the authority's RMP. Most plans are agreed on an ongoing improvement basis and the Keeper will monitor progress over time.

Digital preservation is required to ensure the long-term preservation of digital records. There are different ways of achieving digital preservation, from acquiring an 'off-the-shelf' solution from a commercial vendor, to managing everything in-house using open-source software and existing resources. A balance between the two approaches is also possible.

2.2 Digital preservation top-level guidance

The top-level guidance (this document) aims to help local authorities start planning for digital preservation and look at the options available for the second approach, managing the process as far as practicable within the local authority. It describes an overview of the required procedures using non-technical language and is aimed at the multiple stakeholders who will need to be involved in the process. A case study of the process

(b)include, in particular, provision about—
(i)the procedures to be followed in managing the authority's public records,
(ii)maintaining the security of information contained in the authority's public records, and
(iii)the archiving and destruction or other disposal of the authority's public records.

[6] Supplementary Guidance on Proper Arrangements for Archiving Public Records https://www.nrscotland.gov.uk/files//record-keeping/public-records-act/supplementary-guidance-on-proper-arrangements-for-archiving-public-records.pdf

and system in use at NRS will demonstrate how an inexpensive and simple solution can be implemented to achieve the most critical step of safeguarding the digital records.

2.3 Digital preservation best practice guidance

At a later date in addition to the top-level guidance there will be a longer, more technically detailed document that describes the process in more detail and sets out best practice. This will be aimed at the members of staff who are tasked with the detailed implementation and management of digital preservation.

2.4 Digital preservation capacity planning tool

Accompanying the top-level guidance document is the Capacity Planning Tool, produced to assist in estimating the quantity of digital records that the local authority will need to manage and keep permanently.

3. Getting Started

The start of the process will involve information gathering and forming a network of stakeholders from within the authority. One of the most important factors in making a successful start with digital preservation will be establishing ongoing relationships between these stakeholders. A strong relationship between the archives and records staff and the ICT staff in particular, will contribute to the success of digital preservation planning.

3.1 Key internal stakeholders

The key stakeholders within the local authority for the digital preservation planning process will likely have responsibility for the following functions. Some of these roles may be combined or split amongst different individuals:

Archives: This role has responsibility for the permanent preservation of records, identification of records of historical value and making records accessible to the public

Records management: responsible for the organisation and management of the local authority's current, recently active and inactive records

Information governance: responsible for information policy, legal compliance and security

Business management: performs business analysis and ensures adherence to local authority goals

ICT: responsible for technological systems infrastructure and support

Procurement: purchases and licenses necessary equipment and infrastructure

The people performing these roles will have valuable insight into the requirements for digital preservation planning within the local authority.

It is likely that some of the existing systems and processes can be put towards performing the necessary actions for digital preservation. Having a comprehensive knowledge of existing processes increases the likelihood of successfully making use of these. Previous business analysis work may be put to use at this stage, particularly if focussing on records, such as may have been conducted by the records management department.

3.2 External stakeholders

Collaboration with other local authorities

Scottish local authorities all have the same function: to provide services for the people of Scotland. While services and the means of delivering them vary, authorities may find there are benefits of collaborating with other local authorities who are also dealing with the same need to prepare for digital preservation.

Some of the digital record keeping systems in use, such as certain Electronic Document and Record Management systems (EDRMs) are common to several local authorities; in the case of the Education system, SEEMiS, it is common to all of them. This commonality of systems could benefit from a collaborative approach towards the archiving and permanent preservation of these records.

Sharing knowledge and experience with other authorities may be more effective and lead to finding a solution more efficiently. Consistency in approach is also likely to be beneficial to external stakeholders managing or engaging with the common systems.

3.3 Further assistance

Creating a digital preservation process will require the staff involved to have specialist knowledge. They will all need basic knowledge of digital preservation and some may benefit from more detailed knowledge. This can be achieved by training existing staff, or by recruiting staff who already have those skills.

There are organisations which run training courses and offer advice about digital preservation.

The **Digital Preservation Coalition (DPC)** holds many events, often in Scotland, and provide online training materials and advice.

National Records of Scotland (NRS) provide advice and support for local authorities meeting their obligations under the Public Records (Scotland) Act 2011 and will also be providing advice and support for digital preservation.

4. Planning

4.1 An overview

A top-level view of the digital preservation process has five stages. The immediate priority are stages 1, 2 and 3 which cover the capture and storage of digital records. The later stages covering access to records can be planned in detail after the data is secure.

Stage 1. Analysis and planning

This will involve assembling the key stakeholders and working out the key requirements for the local authority. Questions to ask are:

- How many digital records will need to be stored?
- What are the storage requirements?
- What formats are the records in?
- Are there systems at risk?

Stage 2. Storage

The security of the storage must be appropriate to the content of the records. Records that are closed or containing sensitive personal information must be stored at a level of security appropriate to the classification. There may be more than one level of security required for the storage of digital records.

Best practice for digital preservation is to store three copies of each record. This means the storage system should have managed back-ups, including location and media variation. This means having storage in more than one physical location, for example in different towns, and in more than one type of system, such as on digital tape and also on a cloud service. This will be part of the authority’s business continuity plan.

The long-term viability of the storage must be assured; short- or medium-term contracts with a third party must be considered carefully for suitability to safeguard the data for decades, and control over the data must be retained. Any storage system is unlikely to last the full period of time the data must be stored because most technological systems become obsolete at around ten years, so it is essential that an exit strategy including transition to a subsequent system is accounted for when planning for the initial system.

Stage 3. Capture

Before accepting the data, it must go through several processes, including a process to make sure it is virus free. Each digital record is analysed and given a digital status report, which is used from then on to check that the digital record remains unaltered. This ensures the integrity of the data.

Information about the record is included as metadata and becomes part of the record. This can be gathered using a simple analysis tool, such as the free software DROID. This analyses the record and creates a report on descriptive data such as file format, file size and other basic information.

Once this has been done, the record is captured in storage. This is the critical part of the digital preservation process – without the secure capture and storage of digital records the later stages of analysing the records in detail and making them publicly accessible cannot happen. For this reason, **NRS recommends that the focus remains on these first three stages of capturing the digital records at the start of the process**.

Later stages:

Stage 4. Detailed data analysis

When the digital record is captured, you may only have basic information about the contents. This should not prevent the capture of records, as a more thorough analysis can be conducted on the records at a later date.
The volume of digital records requiring preservation may mean that existing archival processes of accession and cataloguing may not be possible at the point of capture. The information gathering part of these processes may need to wait until resources are available to conduct them. It may be that there is unlikely ever to be enough spare capacity within the human resources available to undertake these processes; fortunately, technological advances are happening at a pace where it is possible in the future for much of this work of information gathering and analysis to be automated.

Stage 5. Accessibility

Ultimately public records need to be accessible to the public to fulfil the function of a local authority archive and adhere to the values of transparency and accountability. Again, the technological solution to manage this may not be in place at the beginning of your digital preservation process, but having the data stored securely will give you the option to find the most appropriate access solution and implement it when ready. As illustrated by the NRS case study, interim solutions include copying files to a drive and giving access in a search room.

4.2 Digital preservation is an ongoing commitment

Digital preservation is an ongoing process and will need continuing resources. The process will
need to be sustainable and supported.

While starting the digital preservation process may require setting up a project to establish new systems and working practices, the process itself must become part of the authority's 'business as usual' and the responsibility for it migrated into the ongoing work of the local authority.

5. Storage

5.1 Storage capacity

Permanent storage will be needed for all of the local authority digital records that are to be kept permanently. This will include 'born digital' records, those created in electronic systems, and digitised records, those imaged from paper records.

Working out how much digital storage will be required will need some analysis. It is unlikely to have a direct correlation to the number of paper records permanently preserved for many reasons; among which are that greater quantities of data are being collected in digital systems than in paper systems, and much of this data may have value for future generations.

NRS has produced a Capacity Planning Tool to help local authorities estimate their requirements for storage. The tool is based in Excel and is simple to use; entering various details about the digital records currently being used and answering some questions will produce an estimate of the storage that will be required, which can then be used as a baseline in discussions for planning of storage.

5.2 Type of storage

There are several different options for storage. You may decide that a combination of storage is most appropriate, particularly when thinking about the long-term resilience of the data. It is recommended that there are three copies of each digital record, stored in different locations.

Servers:

Existing local authority servers will already contain digital records. It may be possible to acquire new server space dedicated for the permanent preservation of digital records. This scenario is explained in more detail in the case study for the NRS Interim Solution. Commercial vendors may offer server storage. With any third-party service it is important to ensure the appropriate level of security is obtained.

Tapes and discs:

Most back-up systems use digital tape or discs.
Commercial or third party operators may offer digital tape or disc data storage.

Cloud:

Cloud providers use servers and tape drives to store data.
Currently most cloud providers are commercial vendors, many are from overseas. For cloud storage it is particularly important that data protection regulations are complied with as some data may not be able to be stored outside of the United Kingdom or the European Union.

6. Capture

6.1 Digital records for permanent preservation

This process of appraisal for digital records will be carried out by staff working in the records management and archival functions of the local authority.

6.2 Checking the data

Digital records can be delivered to the archive using various delivery methods. The transfer method should be appropriate to the records being transferred. Some records will need more secure delivery than others.

At the delivery acceptance stage all records must be:

- Notified to archive ahead of delivery
- Checked for viruses
- Given a digital ‘fingerprint’ called a ’checksum’ on receipt which can be checked periodically to ensure the digital record has changed at any point
- Analysed to ascertain size, format and other attributes.
- Stored securely

There are many open source tools available for free from reputable organisations, such as The National Archives, which can manage parts or most of this process. An example of this is DROID, a program that will analyse the record and provide and validate the record metadata.

7. Maintenance

7.1 Data integrity

Data should be checked periodically to ensure the integrity of the digital records. Using the data collected at the time of the record’s acceptance, checks can be made throughout the life of the record in the storage system to make sure nothing has changed in the form or content of the record.

7.2 Digital record audit trail

Any action involving the digital record will be recorded and added to the metadata for the file.

7.3 Detailed record analysis

Once the data is secure it may be possible to analyse the record’s contents beyond the basic information captured at the initial stage before being ingested into the storage system.

8. Access

This is the final part of the digital preservation process. Making the records available to the public and to internal users is the purpose behind the whole process and fulfils one of the most important functions of a local authority, being transparent and accountable. The system for making records available ultimately may take years to put in place.

8.1 Making the records accessible in the short term

Once the data is secure, a simple and low key system for accessing records can be in place immediately. This may involve transferring files onto a portable drive and making them accessible in a local search room. While this may not be the most efficient way of making records accessible, it provides a method of meeting the obligations of accessibility to both internal users and the public.

8.2 Making the records accessible in the long-term

Over time, the requirements for a system to make records accessible will become clear. It is not necessary at the beginning of the process to try to think ahead to the end result, as this may cause delays in getting started on the most critical stage of capturing and storing the digital records.

Once this first part of the process has been achieved, resources can be diverted to thinking about how the records may be served to users, including the public.

Factors that may be considered at this later stage include:

- Formats used for access copies
- Catalogue
- Copyright
- Redaction of sensitive content

It is likely that much of the management of the content that is served up to the end-user can be automated in future.

Case study

NRS are running a digital preservation programme to establish the systems and processes needed for the permanent preservation of Scotland’s digital public records. Until these systems have been fully implemented, NRS are using what is termed the ‘interim solution’, which allows NRS to safely and securely process and store transfers from depositing organisations. This can be replicated with the following components by any local authority wishing to begin digital preservation. Each local authority may adapt these processes to their own requirements.

The interim solution consists of:

1. Secure storage space on a networked server
2. Encrypted portable media to transfer digital records from depositors to the secure network
3. A standalone (non-networked) computer with write blocker
4. Software to run some archival and technological processing before ingest
5. An archivist to manage these systems and processes

1. Storage:

The storage space is a dedicated secure space for the medium term storage of born-digital archival records. This space was allocated for this use after a period of negotiation with NRS’s ICT department.
ICT assigned space on a server which is primarily used for a different purpose. The level of security for the server space is determined by the sensitivity of the records. Access to this portion of the server space is limited to a small number of staff to maintain security.

2. Portable media

Depositors transfer their selected digital records on an encrypted portable USB drive, supplied by NRS. The drive also includes details of the records contained on the drive. The drive is used to copy the records to the standalone computer for processing, and finally to transfer the records to the server.
Where access to records is requested, portable media can be used to transfer the records from the secure server to a terminal at which it can be accessed, for example in a search room.

3. Standalone computers

Any time removable media is connected to any pc or other network device this should be done using a write blocker in order to protect the integrity of the data on the device. The write blocker acts as a valve which prevents the computer from kaing any alterations to the content of the drive.
A standalone Windows PC is used to quarantine the digital records and run software to check they are virus-free. It is essential that this is done before anything else so that any virus or malware does not infect the rest of the business by accessing the network. This computer does not run any software except for the basic operating system and virus/malware software. If a virus is found then the depositor is requested to send a complete new copy of the digital records and the process repeated. The PC is cleaned down before re-use.
Security updates are managed by ICT. New virus definitions are sent to the digital archivist on portable media, who then installs them on both computers.

4. Software for pre-ingest processing

Several archival and technological processes are run on the records before they can be ingested onto the dedicated server. NRS run this software on a second standalone computer to isolate the digital records from the network. Again a write blocker is used and the processes are run over the data while it remains on the hard drive.
A software tool called DROID is used for file identification and creates a report of the precise file format of each record. DROID was developed by The National Archives and is available to download free from their website:
http://www.nationalarchives.gov.uk/information-management/manage-information/preserving-digital-records/droid/

DROID is also used to create a checksum, a unique sequence of letters and numbers which is a kind of digital condition report. If the digital record changes at all, the checksum will also change. Checksums will be checked periodically over the life of the digital record to demonstrate its integrity.
Once the records have been transferred to the server DROID is run again, mainly to generate a new set of checksums; these are compared with the first set using Microsoft Excel to ensure no changes have occurred within the records as part of the transfer process.

5. Archivist

At NRS the archivist is a designated digital archivist, but it could be an archivist with digital skills. The digital archivist within the Digital Records Unit at NRS is responsible for all of these processes. Currently these processes are manual and require the knowledge and experience of an archivist to ensure that they comply with best practice and existing NRS policies.

NRS does not currently have a cataloguing schema in place for use with digital records, which will in future provide a means for assigning reference numbers to records, and so the accession number allows for a clear and simple method of identification for processing and storage. While this may not be the best way of managing these records long term, it avoids having to create a new system of referencing at short notice which may not be suitable in the future.

The digital archivist also carries out pre-ingest processes, transfers records to the server, and provides access to records as required.

While this process is highly manual, it is inexpensive and practical in developing the systems and processes necessary for digital preservation. It provides a valuable opportunity for learning how the various processes interact. As the programme scales up and becomes more automated, manual intervention will become less necessary. The interim solution will be phased out but will have served the purpose of providing digital preservation for National Records of Scotland until a more cohesive and technologically sophisticated system is implemented.

References:

Digital Preservation Handbook, 2nd Edition, http://handbook.dpconline.org/, Digital Preservation Coalition © 2015

The National Archives Digital Preservation Tools (downloads including DROID on TNA website) http://www.nationalarchives.gov.uk/archives-sector/advice-and-guidance/managing-your-collection/preserving-digital-collections/digital-preservation-tools/

Glossary:

Access Continued usability of the digital record

Accession The process of accepting a deposit of records into the archive

Audit trail Documentary evidence of the sequence of activities that have affected a record

Automated The management of a process without human intervention eg by algorithm

Back up The copying of files to a secondary site and alternative media for preservation in case of equipment failure or other catastrophe

Born digital Digital materials that have not been converted from a non-digital format and have no analogue equivalent

Business continuity plan The process for anticipating threats to the business and planning for recovery to return to business as usual

Capacity Planning Tool Excel-based tool developed by NRS used to estimate digital preservation storage needs

Capture Collecting and storing digital information or records

Checksum A unique numerical signature derived from a file, against which later comparisons can be made to detect changes or errors in the record

Cloud storage A storage model in which data is stored on remote servers accessed via the internet. It is usually maintained, operated and managed by a service provider.

Copyright A legal right that may affect how some digital records are processed or made accessible

Digital preservation The series of managed activities necessary to ensure continued access to digital materials for as long as necessary

Digitise The conversion of non-digital text, pictures or sound into a computer readable format

Drive A data storage device

DROID A file format identification tool developed by The National Archives

EDRMs An electronic document and record management system

Exit strategy A plan for getting data out of the current system at the end of its life

File A piece or segment of digital information

Format A documented, standard way that information is encoded for storage in a computer file

Hardware The physical element of computers, servers and other components of a technological system

Ingest Capturing, importing and transferring data

Integrity The accuracy and consistency of stored data

Interim solution The system in use at NRS to manage the initial stages of digital preservation

Legacy system Non-current computer system that may still be in use and/or contain data that needs to be preserved

Metadata Information that describes the digital record, or descriptive data

Network A computer system where the computers are linked in order to share information and services

Non-networked A computer that is not linked to any other computer or system thereby making it secure from viruses

Off the shelf A product that is purchased ready to use, not tailored or designed for specific requirements

Records Management Plan A plan required of all named Scottish Public Authorities under the Public Records (Scotland) Act 2011, detailing the proper arrangements for the management of the authority's records

Standalone A computer or device not connected to any other

Transfer The movement of digital information from one device to another

Transmission The delivery of records from a depositor to an archive. Includes transfers to an archive within the same organisation.

Writeblocker A hardware or software component that prevents the contents of a drive being changed.