Archives First: Digital preservation project

Viv Cothey * and Cassandra Pickavance **

2017

* Gloucestershire County Council and University of Wolverhampton
** Dorset County Council and Dorset History Centre

Contents

Executive summary page 1

Introduction page 3

Methodology page 7

Findings page 9

Discussion page 19

Conclusion including recommendations page 27

References page 31

Appendices page 33

- Members of the Archives First consortium
- Project funding proposal
- Disaster recovery versus digital preservation
- Survey instrument
- Local authority software applications: RM1059
- Digital continuity policy

Disclaimer

The views and opinions expressed in this report do not necessarily represent those of the institutions to which the authors are affiliated.

Acknowledgement

The project was partially funded by The National Archives, UK.

Executive summary

Archives First is a consortium of eleven local authority records keeping services across the south of England.

During late 2016 and early 2017 Archives First undertook a project to determine what added value archivists could provide in the context of so-called “digital working” since digital working “...completely change[s] the concept of information and records, as well as what constitutes effective information management” (Cabinet Office, 2017, p6).

In an era of fake news, users trust the integrity of information managed by archivists and rely upon it “...to hold government and organisations to account...” (The National Archives, 2016).

The project aims to understand how this trust can be maintained into the future and in particular to identify how archivists can contribute to the long-term management of preserved digital material.

Following a survey of the eleven local authorities into how digital working has affected the way that information is now created, the project concludes that:

- an urgent paradigm shift is needed that focusses local authority archivists' attention on the *long-term* preservation of information in digital format rather than on their traditional role relating to the *permanent* retention of information,

- Archives First should influence the debate within the archives and associated information technology communities regarding the long-term management of digital material,

- the current generation of computer systems developed to provide for digital working has ignored the need for the long-term archival preservation of information. It is vital to recognise that most information is now assembled temporarily from disparate items of structured data and does not exist as a (digital) document entity.

- Archives First should emphasise the intellectual added value of the catalogue which is much more than a mere list of contents. It is the organisational and descriptive power of the catalogue that underpins the achievement of archival provenance and integrity.

There are four recommendations:

1. archivists should adopt a leadership role in respect of issues connected with the long-term preservation of digital information. In particular they should engage with both information asset owners and technologists to become involved in system procurement. They should also identify all information which is to be retained for ten years or longer.

2. individual archivists should exploit opportunities to become familiar with digital preservation issues, terminology and practice by, for example, supporting small scale digital preservation projects and providing training opportunities. Innovative practice should be shared within Archives First and more broadly.

3. Archives First should carry out a follow up project to investigate archival information package export specification and functionality in respect of:
    a) Liquidlogic Children's Social Care System (i.e. adoption cases), and
    b) modern.gov (i.e. committee minutes).

    (Archival information packages provide the basis for long-term information preservation.)

    It is anticipated that the investigation here will include liaising with archivists in Scotland and will support further work aimed at specifying mandatory functional requirements to be included in future local authority system procurement exercises.

    It is also anticipated that the outcome of such an investigation will be shared with other relevant consortia.

4. Archives First should carry out an investigation to determine the minimum requirements of a long-term storage system for archival information packages and identify available options for local authorities. It is anticipated that the outcome of such an investigation will be shared with other relevant consortia.

1. Introduction

Archives First is a consortium of eleven records keeping services that shares best practice and opportunities for collaborative investigation. The consortium members are local authorities located across the south of England (see Appendix one).

“Digital preservation” was identified as a priority topic. All consortium members are already experienced in at least some of the processes involved when accessioning digital material. Such material is currently the result of, for example, community projects and oral history research.

The need to establish digital preservation capacity and skills development has been long recognised both generally and within the local authority sector. However previous investigative work has concentrated on preparedness and building an awareness of a variety of potential technological challenges relating to the long term preservation of digital records.

There is also now a focus on the benefits of digital preservation (The National Archives, 2017a).

This project has a practical focus. It attempts to carry out a life-cycle analysis of so-called “born digital” records from their creation through to their accession. This is in order to understand how archivists can contribute to the long-term management of preserved digital material. In particular, the project seeks to identify the key roles where archivists can add value.

While access to records is an important part of their life-cycle, the project focusses on creating, managing and preserving material.

The record classes of interest to the project were:

coroners courts,
democratic services that is committee meeting minutes,
planning and building control,
social care, particularly adoption, and
magistrates courts.

In addition some investigation of electoral registers was also undertaken.

The project received funding support from The National Archives. A redacted version of the funding proposal is shown in Appendix two.

Local authorities have been required to adopt digital working practices as part of a general transition to “e-government”. In consequence most record creation is now undertaken by a computerised transaction processing system. These systems facilitate delivering an efficient service to a service user as well as, for example, automatically collating the service history of a service user which can be thought of as a “case file”. The project's investigation identified that all the material of interest was (or soon would be) created by a computerised transaction processing system.

Five important features of a computerised transaction processing system were identified:

procurement,
exit strategy,
migration strategy,
export process, and
disaster recovery plans.

These are introduced here in order to provide a backdrop to the project. In particular the project's investigation and life-cycle analysis emphasises the importance of the export process.

Procurement

Computerised transaction processing systems are purchased/leased software products that together with support contracts are obtained through a procurement process. The procurement process is regulated and contracts have a limited duration, typically five years. Contract extensions and re-engagement is restricted. In addition any particular software product will have an end-of-life which also limits the duration of software support, for example to provide software maintenance and fix security vulnerabilities. In practice the life of a product may be determined by the life-cycle of pre-requisite software such as operating systems or database products. (For example, mainstream support for Windows 10 ends in 2020 with extended support finishing in 2025. Oracle provide extended support for their Database (version 11.2.0.4) until 2020).

Exit strategy

An exit strategy is needed in order to safeguard the transaction processing data held by the system when the product is either terminated or upgraded/replaced. It cannot be assumed that a supplier will support an orderly end-of-life migration to a replacement system. This significance of exit strategies is discussed in UK Government (2012 and 2015).

Migration strategy

A migration strategy is a particular version of an exit strategy that will almost certainly require the cooperation/technical assistance from experts in each of the suppliers in order to support the orderly replacement of an existing system by its successor system. The difficulties of achieving systems migrations from one supplier to another causes supplier “lock-in”. The importance of avoiding supplier lock-in is discussed in UK Government (2012 and 2015).

Export process

An export process provides a mechanism to collate otherwise disparate transaction processing data in respect of, for example, a completed case. The collated information can then be “exported” from the system in a form that does not require any further access to the system in order to interpret it. The export process should be used routinely during the lifetime of the system in respect of information that is no longer operational.

Disaster recovery plans

> Disaster recovery planning supports recovering the system to an operational state following a natural or human induced disaster affecting its operation. This often involves “archiving” backup copies of data. Despite similarities in terminology and some procedures, disaster recovery and digital preservation are separate activities (see Appendix 3 for more detail).

The project's investigations did not extend to corporate policy documents. However, it is noted that relevant policy documents are probably out of sight of archivists in unmanaged systems, for example shared computer hard drives. The “Better information for better government” report discusses this issue (Cabinet Office, 2017). “Better information for better government” makes two other salient points. Firstly that;

> “[Digital working] has completely changed the concept of information and records, as well as what constitutes effective information management.”
>
> (p. 6)

and then;

> “Technology solutions have historically been designed without considering the information management consequences...”
>
> (p. 21)

The rest of this report comprises four main sections:

methodology,
findings,
discussion, and
conclusions including recommendations.

There are six appendices.

The project team members were (in alphabetic order), Claire Collins, Viv Cothey, Julie Courtenay, Roz Farr, Heather Forbes, Sam Johnston and Cassandra Pickavance.

The investigation's methodology is described in the next section of the report.

2. Methodology

The intended analytic method was to compile life-cycle flow diagrams for paper based records and for born-digital records in respect of each of the record classes mentioned earlier, that is:

coroners courts,
democratic services, that is committee meeting minutes,
planning and building control,
social care, particularly adoption, and
magistrates courts.

There was also an opportunistic investigation of the deposit of (digital) electoral registers since Gloucestershire Archives already had experience of accessioning examples of these records.

It was anticipated that investigation and a detailed comparison of analogous events in the record life-cycles would reveal how archivists could work with future records.

The project's initial data collection phase was a structured email and telephone interview survey of respondents from each of the eleven consortium members. The survey instrument is shown in Appendix four. It was tested and refined by a pilot study involving three of the consortium. Each of the eleven consortium members had been pre-assigned two or more examples from the record classes noted above, (see Appendix one). These were investigated in detail as well as there being questions about their local digital preservation situation more generally.

This survey investigation revealed that there was a general issue regarding record life-cycles where computerised transaction processing systems were now in use. That is everywhere!

The survey also revealed that consortium archivists could not obtain essential information such as information export capability that is needed to plan the future preservation of information.

Given the ubiquitous and central role of computerised transaction processing systems a follow up data collection exercise was undertaken. This exercise was an email based questionnaire survey (see Appendix six) of the nineteen systems suppliers advertised by the Crown Commercial Service. These were chosen as being the principal suppliers for business systems supporting the record classes being investigated.

In addition to the intended record class by record class analysis the project now refers also to a generic model life-cycle applicable to paper based record systems, (see Figure 6).

This generic life-cycle is compared with a similar generic model life-cycle for a computerised transaction processing system (see Figure 7).

This comparison of the contrasting generic life-cycles is discussed in section four of the report.

The investigation's findings are set out in the next section of the report.

3. Findings

The project aims to identify how archivists can contribute to the long-term management of preserved digital material. In particular, the project seeks to identify the key roles where archivists can add value.

This section is in four parts. Firstly we report on life-cycles for born-digital material, that is material created in a computerised transaction processing systems. In section four, next, we compare a generic life-cycle for born-digital material to its paper based equivalent. This shows that the required system support for preserving material is missing. That is, future records will not "cross the archival threshold" (Duranti, 1996).

Secondly we report how archivists are pursuing their traditional roles and responsibilities in respect of born-digital material. Archivists have, as yet, been unable to influence system design to facilitate the preservation of future material.

Thirdly, we report on the system suppliers and digital preservation. It appears that the long-term preservation of material is not a system requirement. It appears not to be supported.

Lastly we include a record class by record class commentary on the survey responses from consortium members. This includes findings in respect of electoral registers since the experience of the British Library is particularly instructive.

3.1 Record life-cycles

The findings here are based on responses to sections B and C of the survey (see Appendix four) which addresses the particular record classes assigned to the respondent (see Appendix one).

Material is being created and managed electronically in all cases although there are some hybrid electronic/paper systems (for example, Coroners courts and where a physical signature is required).

Where immediate public access is required (for example, committee meeting minutes) this is achieved by a variety of web publishing techniques.

Respondents generally experienced difficulty finding out detailed information about system functionality as requested since this relied on some degree of technical support.

In most cases data for the record classes concerned is hosted on equipment managed or owned by the local authority.

In several instances it was reported that relevant systems were subject to to a current procurement.

Only one respondent reported that it was thought that the system in question could export non-operational material although this functionality is unspecified and untested.

It was reported that data is not encrypted at rest. The reverse, that is data at rest being encrypted, is antithetical to long-term preservation.

No documentation regarding exit strategies was available although some were said to exist.

With one exception, material that is being created and managed electronically is not being exported to a records management system. In the time available it was not possible to investigate any of the details of the exception but see section four regarding Figure 8. Equivalent paper records generated by systems that are currently hybrid are transferred but on an ad-hoc rather than a routine basis.

Respondents cited several barriers to accessioning material for long-term preservation, including,

change resistance by the business and a lack of interest in the needs of the archive,
security concerns by the business,
an ignorance of technology coupled with the belief (by the business) that IT are taking care of long-term preservation,
at least 100 years retention is not permanent (therefore not archival),
lack of knowledge of procurement processes and how to get involved, and
lack of clarity over responsibilities (especially in relation to Coroners' records).

3.2 Archivists' roles and responsibilities

The findings here are based on responses to section D of the survey (see Appendix four) which addresses the role of archivists with respect to “long-term” preservation.

Respondents saw no distinction between “permanent” and “long-term” which was suggested to mean between 10 and 20 years. Almost all wanted to be involved in the design and creation of business systems at the earliest stage possible.

There was a range in the closeness of the relationships between “archives”, and “records management” but a strong consensus that it was difficult to establish a relationship with IT that addresses the issue of long-term preservation. Reasons suggested for this included the effects of outsourcing and a lack of confidence by archivists to engage with IT.

There was a general view that archivists should adopt custody of material as soon as possible after it was no longer in current use. However “custody” in this context was not defined.

Determining the reach of the archive “catalogue” divided respondents. There was a view that only material within the direct custody of the archive should be included within the catalogue. However the consensus appeared to be that the catalogue should show the location of relevant material, wherever that might be.

Views more generally (for example, Webb, 2017) identified that the catalogue was a key added value component of the archive. The catalogue is not a mere list of

content. It is the organisational and descriptive power of the catalogue that establishes archival provenance and which engenders the users' trust in the integrity of the archive.

3.3 System suppliers

The findings here are based on the eleven responses to the email based survey of system suppliers (see Appendix five) which addresses the capability of systems with respect to “long-term” preservation.

There was a general reluctance to make an explicit statement regarding system end-of-life. Most responses regarding future support appeared to be marketing led and simply claimed to meet customer requirements. However reference was also made to procurement cycles and ten to twenty years contractual periods. It was also noted that current and previous versions were always supported (but no information was given about the upgrade frequency).

Only one supplier made reference to the need to retain records for longer than the lifetime of the system. The response from this supplier also appeared to show a reasonable understanding of the Data Protection Act, 1998 (DPA) and the need for “export”.

Most responses made reference to retention schedules and the DPA. It appears that suppliers expect customers to retain information within the system just for the duration of the retention period and then to delete the information.

Several responses also referred to specific tools which would allow a customer to extract information but details were scarce. Two responses referred explicitly to SQL (Structured Query Language) databases while another says “records can be exported as a set of tables”. This is not sufficient to provide for long-term preservation.

One response says that the system has an option to archive non-operational records using standard back-up techniques. This also is not sufficient for long-term preservation.

Tellingly, another response was that the supplier had been asked to tender for an archiving tool but that this was not pursued.

3.4 Survey responses by record class

3.4.1 Coroner's inquest records

See Figure 1 overleaf.

Three archive services undertook a study of inquest records. Where some records were being managed digitally the paper version was still considered the master copy. However in all cases a re-procurement was in progress with the intention of moving to a fully digital system.
The IRIS database was used to manage metadata relating to the files. Paper

inquest files were typically transferred to the archive service for permanent preservation at the end of their fifteen year retention period. For two services the metadata was used as the basis for entries in the archive catalogue.

Requests for access to information contained from inquest files under 75 years old are managed by the Coroner's Office.

Two coroners' offices keep audio recordings relating to court activity - either evidence gathered by the court or recordings of inquest hearings. Guidance issued by the Chief Coroner's Office states that such recordings must be kept for at least fifteen years and must be in a digital format and stored with back-up.

Although there is a national network of Coroner's offices, each Coroner has autonomy over how they manage their information. This means that attitudes to managing records vary from enthusiasm for a fully digital work flow to contentment with the current paper system. The National Archives does not anticipate taking responsibility for the preservation of digital coroners' records due to the decentralised administration of the coronial system.

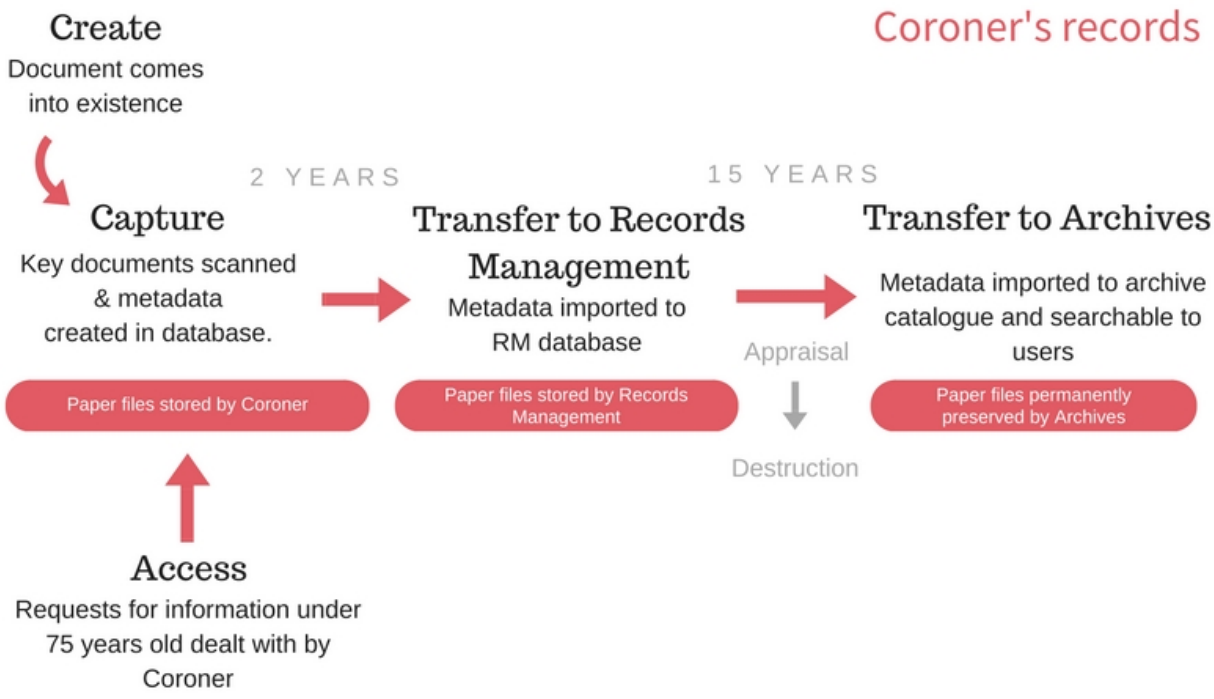


Figure 1: Coroners inquest records

3.4.2 Committee meeting agenda papers and minutes

See Figure 2 overleaf.

Nine archive services reported how committee papers were managed. These covered a range of depositing bodies, including district, borough, county, town and unitary authorities.

Several authorities were pursuing a ‘paperless’ strategy. Councillors were provided with the means to access the papers electronically (e.g. via tablets).

Conversely in one case the authority provides hard copies to every councillor believing this to be a statutory requirement.

Although the view was prevalent that a hard copy version of the minutes must be signed and retained, one depositor said that they could find no legal justification for this. In some instances the hard copy minutes were scanned back into the case management system once signed.

Nearly all archive services received regular deposits of hard copy committee meeting papers from one or more depositing authority.

Hard copy meeting papers were available to view in the archive search room, with access to closed records being mediated by the Democratic Services team. One archive service reported that two depositing bodies had requested to deposit future committee meeting records electronically as a result of communications regarding this project.

Public access to committee meeting records is a requirement for all local authorities. This was achieved in most cases by publishing an electronic copy directly to the council website. The duration for which these records would remain available online varied from “6-12 months” to “indefinitely”. In one instance committee meeting records would be deleted by the IT department when the web servers became full. Several services reported that copies of meeting papers uploaded to the management system were also kept on a network drive as the ‘master’.

The process for extracting committee meeting records from systems such as modern.gov [sic] is not yet fully understood. modern.gov is used by the majority of authorities.

One archive service reported difficulty in identifying master files when working with legacy digital files.

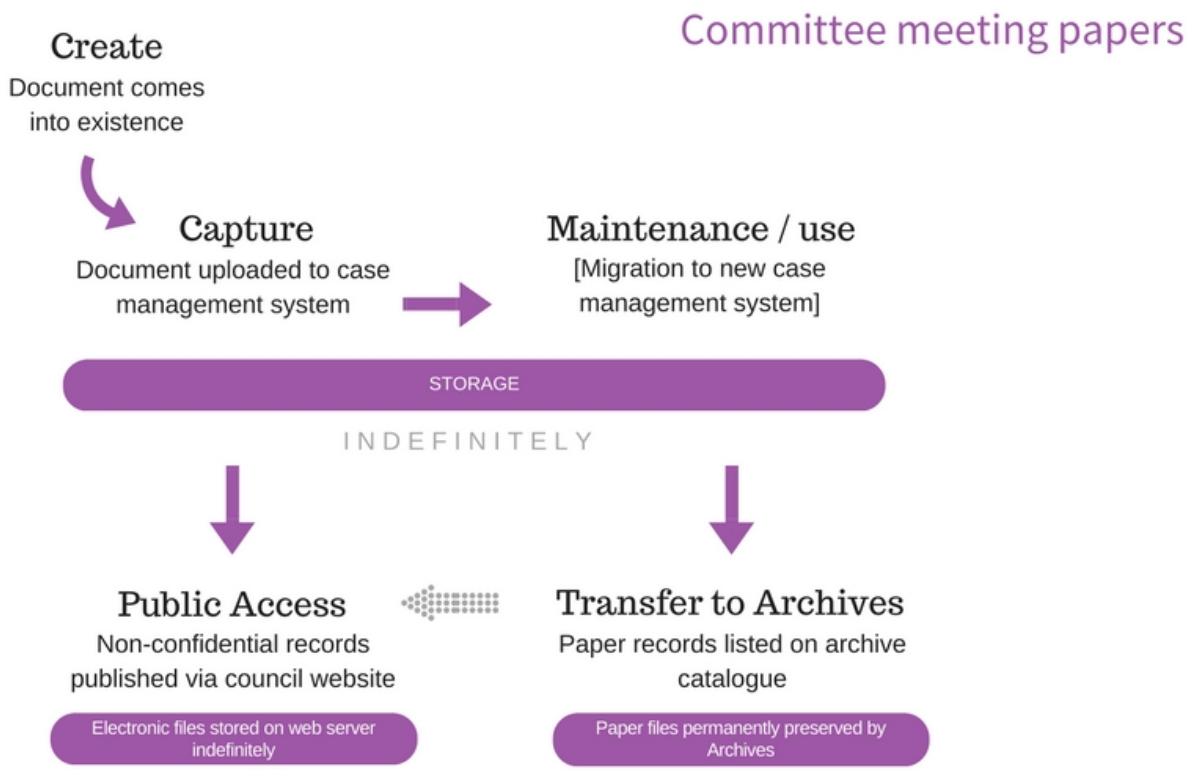


Figure 2: Committee meeting agenda papers and minutes

3.4.3 Planning applications and building control records

See Figure 3 overleaf.

Three archive services looked in detail at the way in which planning records were managed by their depositing bodies. Planning responsibility is complex because of the divisions of responsibility between the County Council and District councils in a two tier system, and between a council and a National Park. The case studies include all of these.

One service reported that there was no retention policy on documents stored in the planning case management system. The intention was to store everything in its entirety, indefinitely. Another planning department intended to scan all paper documentation but to retain only the digital version.

Long-term preservation of digital material had not been considered by the depositing bodies in any of the planning applications and building control records case studies although system suppliers claimed to be able to retain information for over fifty years.

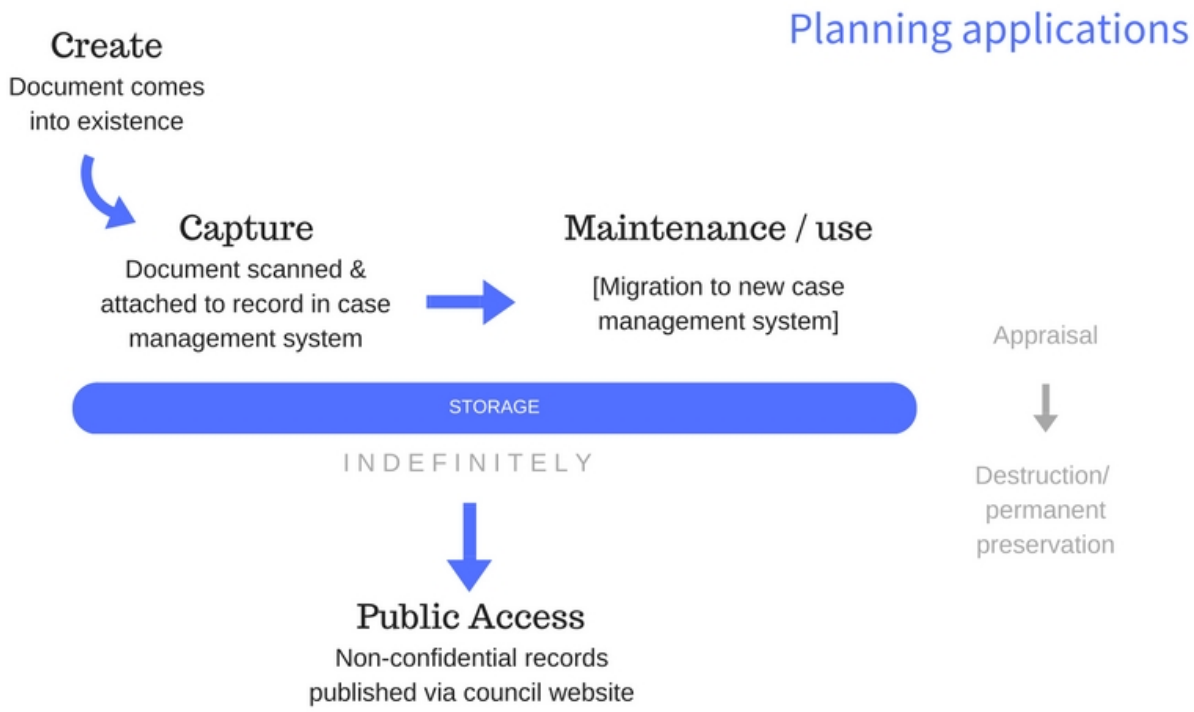


Figure 3: Planning applications and building control records

3.4.4 Adoption records

See Figure 4 overleaf.

Four archive services studied how adoption records were managed. In all instances the social care information management system had either been recently procured or procurement was in progress. Paper documents were routinely scanned and digitised. Documents having sentimental value were retained in their paper form.

Adoption records are noteworthy in that there is a statutory requirement to retain information for at least 100 years.[1]

In two instances either the business and/or IT were responsible for maintaining the records and ensuring their usability.

Two archive services aspire to manage electronic adoption records. However the details are not yet fully understood.

The security of digital records was regarded as an issue by the record creators but maintaining their usability for 100 years was not!

1 Adoption and Children Act 2002, sections 56 to 65 and Disclosure of Adoption Information (Post-Commencement Adoptions) Regulations 2005.

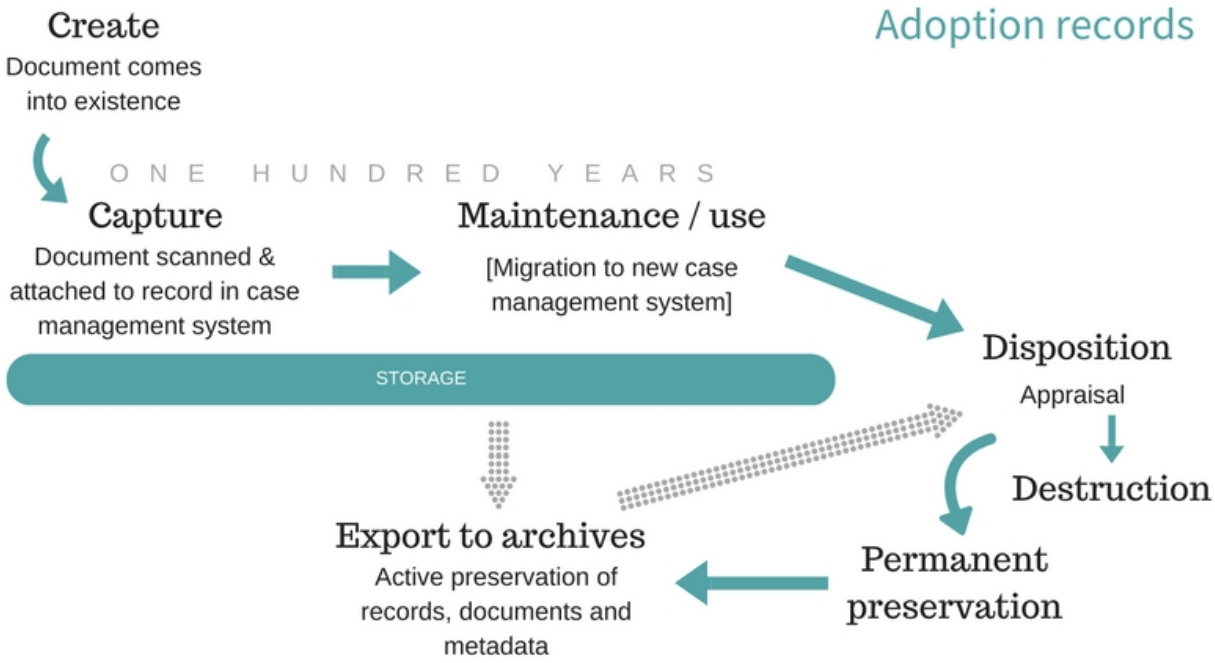


Figure 4: Adoption records

3.4.5 Magistrates' Court records

See Figure 5 overleaf.

Two archive services reported on Magistrates' Court records. All courts in England use Libra with data being stored centrally. The National Archives has indicated that it is likely that they will extract data for preservation although no decision has yet been made. In the meantime The National Archives requires that legacy (digital) data is maintained in a usable form.

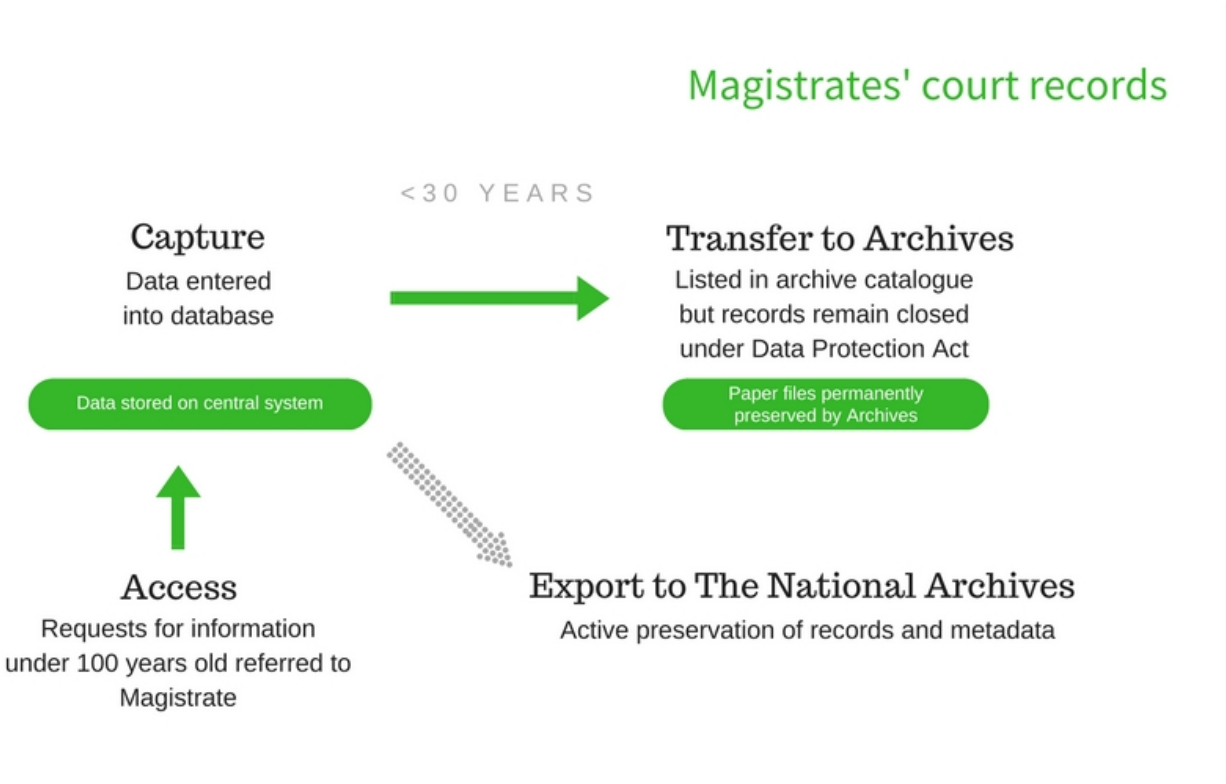


Figure 5: Magistrates Courts

3.4.6 Electoral registers

For several years local districts have submitted electoral registers to Gloucestershire Archives in a raw data format generated as an extract from their electoral registration system. This has provided the archive with an opportunity to gain experience in digital preservation. It was found that access to the extracted material had to be enabled on a case by case basis according to the detailed particulars of the raw data format.

However the same digital material has been collected by the British Library. In order to co-ordinate collecting efforts Gloucestershire Archives investigated their experience. The British Library focus on providing access to the registers and immediately encountered similar problems to those experienced by Gloucestershire Archives but now magnified by the greater national variety of system suppliers' extract formats.

In consequence the British Library have developed an extract format specification and have “contracted with electoral management software suppliers to write code that enables a standardised extract of electoral data from their systems [to be made]. Tests of the code have been successful, and [the British Library] will be asking electoral administrators to begin sending [the Library] standardised data” from December 2017 (Grimshaw, 2017).

The investigation's findings are discussed in the next section of the report.

4. Discussion

In this section of the report we discuss the investigation's findings with the aim of understanding how archivists can contribute to the long-term management of preserved digital material and to identify key roles where archivists can add value.

It is necessary to preserve some information. This may be because of statutory regulation or the need for institutional governance, bureaucratic or democratic accountability. There is also a need to preserve information in order to protect corporate and cultural memory (Cabinet Office, 2017).

All the consortium respondents considered that they should play a central role in the long-term preservation of information, and that they should be involved in this task at the earliest opportunity (with respect to the information). However this is not happening. None of the consortium membership has taken archival custody of material from the record classes investigated (except the instance of electoral registers described above) despite such material having been created and managed electronically for about ten years.

Discussion of the practice of information preservation is often hindered by ambiguous terminology particularly when comparing so called “paper” systems and “electronic” or “digital” systems. For example, the terms “record”, “file” and “archive” carry significantly different meanings depending whether used in a “paper” or “electronic” context.

The Open Archival Information System (OAIS) reference model (ISO 14721:2012) provides a “lingua franca” for discussing the “long-term” preservation of any information, not just “digital information” for which it is essential. “Long-term” is not defined but is generally taken as being sufficiently long to be impacted by environmental/technological change. The OAIS is concerned with preserving information with the objective of being able to access it in the future not with the continuing operational use of information. Clearly though, preserved information can be recycled as part of the information creation process (the so-called information cycle).

A key component identified by the OAIS is the Archival Information Package (AIP) which is a self-contained set of material that contains all the information needed for future access to the “payload” data, that is the material being preserved, within the package.

It is assumed that future material will be accessioned as AIPs and will in consequence appear in the archive's catalogue. However AIPs will not necessarily be under the direct custody of the Archivist. In a so-called non-custodial[1] archival model, storage of material is delegated but the archivist remains responsible and must therefore exercise due-diligence. (Practical examples already exist where, for example, physical material is placed with a neighbouring archive.)

---

1 The orthodox non-custodial or distributed model reverses the Jenkinsonian notion of documents being accepted into official custody and management by responsible custodians. The custody of archival documents is instead entrusted to their originating institution, for example Boadle (2004). Acland (1991) when championing a non-custodial model prioritises the moral defence of the record over its physical record. Critics questioned whether or not the reliability of records could be guaranteed when they are left in the hands of those who are held accountable through them (Duranti, 1996).

Here the non-custodial model is reinvented. The custody of AIPs is not entrusted to the record creators but instead, as necessary, they could be entrusted to a technologically proficient independent third party.

The discussion here considers firstly a comparison between a legacy business system relying on unstructured data, a so-called “paper-based” system, and a computerised transaction processing system that relies on structured data, a so-called “electronic” system.

The discussion also notes several co-lateral issues and opportunities. These are discussed below.

Figure 6 illustrates information flows in a generic “paper-based” system.

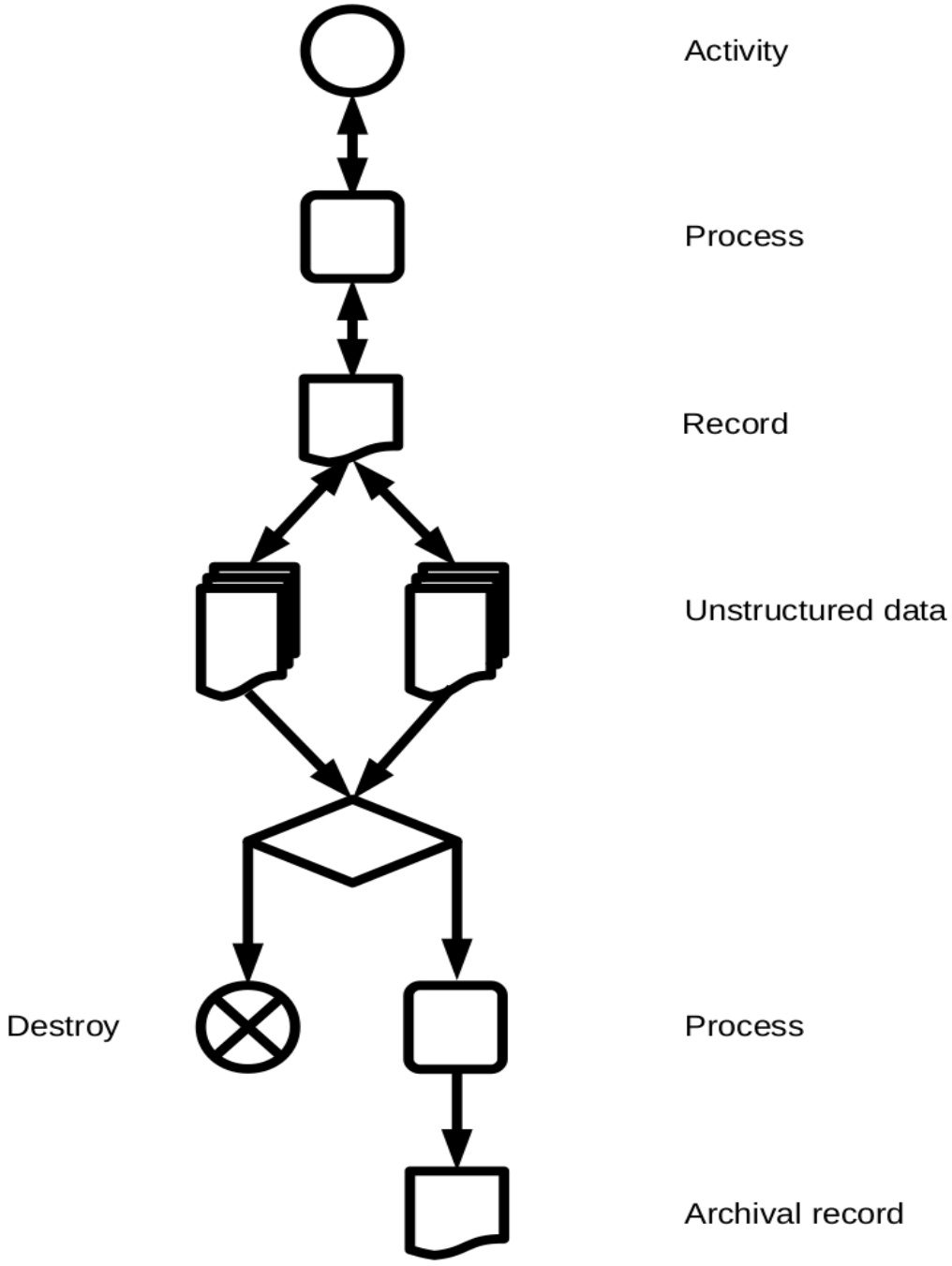


Figure 6: Generic “paper-based” information system

A business activity triggers a business process and vice-versa. Business activities will generally but not necessarily involve people, for example, interviews, surveys, requests etc. The associated process can produce a record containing information. This may rely on information already present in one or more “paper-files”. A record of the process can be included with one or more of the unstructured data paper-files (for example, case files, registers etc.).

When the paper-files are no longer operational they can be physically relocated to be either destroyed or be subject to an accession process that includes them in the archive.

Figure 7 illustrates information flows in a generic “electronic” system.

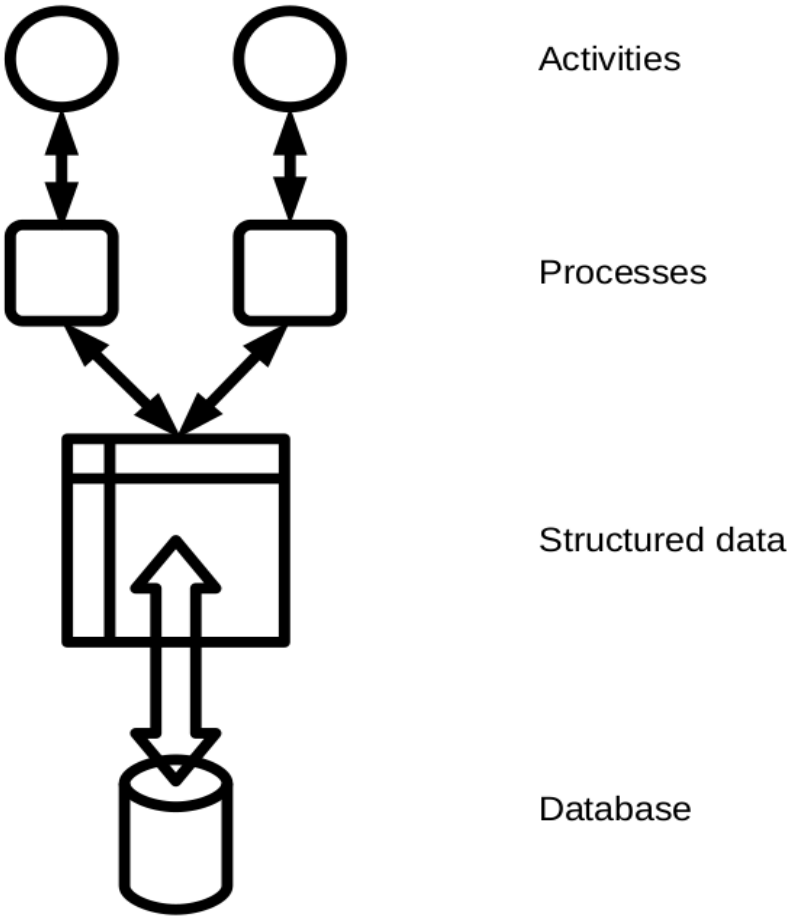


Figure 7: Generic “electronic” information system

As with the legacy paper-based systems people are involved in business activities and processes. However information can now be shared between more than one process. Transaction records in a structured data format can be added to a computer database which can be interrogated in order to support subsequent business processes.

Structured data is often thought of as existing in collections of linked tables of rows and columns. Information is constructed by selectively following the links to combine data from several table cells, that is the intersection of particular rows and columns. Since the tables

in the database are shared there is no analogy to the paper-file in the legacy paper-based system which becomes no longer operational and can be relocated.

In consequence neither information destruction nor archival information preservation is available. Transaction processing data will remain in the database.

How long material should be retained is specified in retention schedules. Inspection of these showed clusters of durations such as seven, fifteen, forty and seventy years. Most of these retention periods are (much) longer than the expected lifetime of any transaction processing system, hence an ever expanding amount of no longer operational data would have to be migrated to replacement systems. At the expiry of the retention period system suppliers provide only for data deletion that is, for example, removing data links so that information cannot be reconstructed. Suppliers appeared to believe that they were obliged by the DPA just to provide for this kind of deletion process. However archivists currently rely on section 33 of the Act, Research, history and statistics, which provides for exceptions to the general rule that data cannot be used or retained arbitrarily, in particular section 33 part (3),

> "Personal data which are processed only for research purposes in compliance with the relevant conditions may, notwithstanding the fifth data protection principle, be kept indefinitely."

(The EU General Data Protection Regulation (GDPR) will come into force 25 May 2018. Article 89 requires that safeguards be put in place in order to protect the rights and freedoms of data subjects when data is processed for archiving purposes for example for public interest or for historical research. In particular data processing must ensure respect for data minimisation. However Article 89 also allows member states to provide so called "derogations" from actions to protect the rights and freedoms of data subjects if these actions are likely to render impossible or seriously impair the fulfilment of the archiving purpose. Consultation in respect of the scope of these derogations in the UK is currently in progress.)

Although no specific classes of records have an indefinite retention period there was a general view that long retention periods should be regarded in practice as being indefinite. In particular respondents considered that information needing long-term (say greater than fifteen years) preservation should be within the archive.

As can be seen from Figure 7, this is not currently possible. In order to achieve an orderly transfer an additional "export" process is needed. This is described below. The goal of the export process is to facilitate creating the AIPs which support long-term preservation.

It is possible to envisage a data extraction procedure that copies material from a transaction processing system to a secondary database rather than exporting material as an AIP. The secondary database could allow for information to be reconstructed, however the same longevity threats and risks that apply to the transaction processing system apply also to the secondary database system. Since AIPs are still required then this double-handling introduces costs and risk.

As described earlier, there needs to be some process that initiates the construction of AIPs from the structured data which supports transaction processes.

Figure 8 illustrates an archival export process in a generic electronic system.

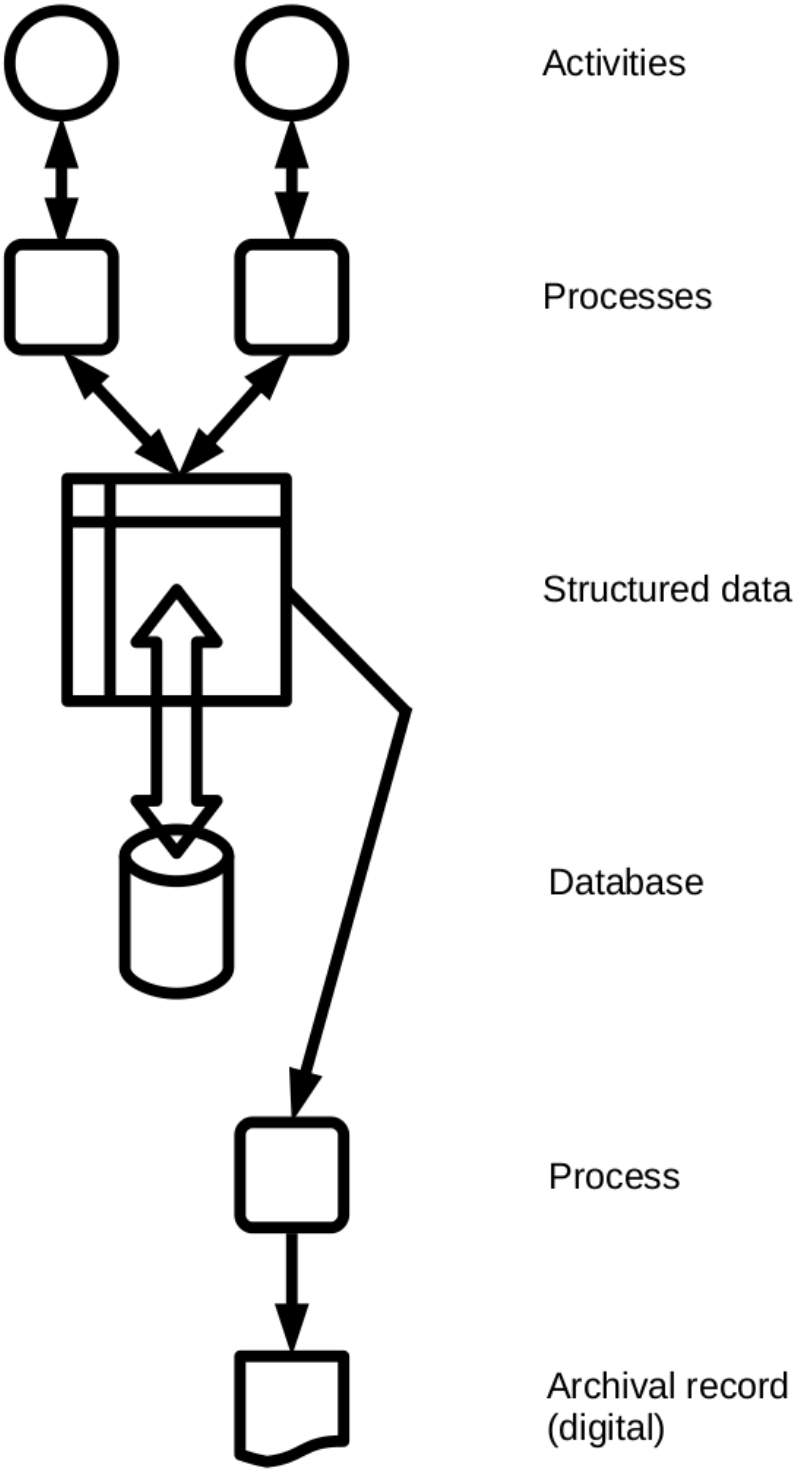


Figure 8: Generic “electronic” information system including archival export

No evidence could be found that the current versions of computerised transaction processing systems in widespread use within local authorities have adequate provision for

exporting archival material for long-term digital preservation.

The exceptional example mentioned above in section 3.1 is thought to be an example of a possible export process. However further investigation of the details involved is needed.

The project team identified several co-lateral issues and opportunities which are noted below. Some of these are interconnected and interact.

4.1 The importance of the role of “information asset owner”.

Each transaction processing system within the business should have an “owner” that takes ultimate responsibility for managing the information asset. This role is emphasised by the GDPR's requirement for privacy by design. The information asset owner plays a central role in the procurement, operation and replacement of the system. Responsibility for the information asset should entail responsibility for exit and migration strategies including archival export.

4.2 Experience of community projects that generate digital material and hybrid deposits.

Digital material, for example photographs and oral history recordings, is already being accessioned by consortium members. In at least one case AIPs are created to package the material. The AIP is referenced in the archive catalogue. Hybrid material, for example a deposit containing digital material, is processed similarly. AIPs, for the time being, are stored as files within the corporate storage system.

The potential copyright issues particularly when working with community projects were noted together with the lack of a general right to copy digital material in order to make back-up copies.[1]

4.3 Policy documents created and stored outwith managed systems.

The situation described for central government in respect of policy documentation (Cabinet Office, 2017) is repeated within local government. It is important that such documentation be specified explicitly within retention schedules.

4.4 Statutory bases

There is no general statutory basis for the indefinite keeping of specific classes of archives. However there are several requirements to retain (digital) material for many decades the longest noted being 100 years for adoption records.[2]

This omission has been recognised in Scotland where it is believed a stronger statutory regime now exists.

Archivists need to review retention schedules particularly in the context of any

1 The Copyright, Designs and Patents Act (1988) is amended by The Copyright and Rights in Performances (Research, Education, Libraries and Archives) Regulations (2014). Regulation 5(2) “42 Copying by librarians etc: replacement copies of works” provides a *qualified* exception to permit *some* copying “in order to preserve...”. However the needs of digital preservation have not been anticipated so that, for example, creating back-ups of protected works *generally* remains unlawful.

2 The longest requested retention period was 125 years in respect of bridge construction.

automatic deletion procedures built into computerised transaction processing systems. Attention needs to be paid to discretionary instances, for example actions such as “records due for review by archivists” can be obligatory.

4.5 The long-term

Archivists' focus of attention should be on the long-term preservation of material and not just on material that should be retained indefinitely. Since “long-term” must now be interpreted in the context of technological change, which is also driven by the procurement cycle, then this may be as short as ten years.

A particular contribution of archivists is an “archival warrant” whereby deposited material remains uncorrupted, in an information sense, once it is accessioned. AIPs are no different except any corruption will be invisible (and probably undetectable until too late). Therefore additional computing measures (i.e. fixity testing) must be put in place in order to monitor the stability of AIPs over the long-term.

The long-term stability of AIPs and the absence of an instant access requirement also means that database systems especially transaction processing systems are not only comparatively expensive but are also inappropriate places to store them. The requirement to provide online access to material (i.e. digital publishing) is outside the scope of the project.

There is a need for a simple and cheap digital preservation equivalent to the traditional archive strong room. It is probable that a long-term preservation system thus envisioned would be part of a non-custodial archival model.

4.6 Twenty-first century “appraisal”

Currently “appraisal” is a decision whether material is deemed to qualify either for retention in perpetuity or not.

The rationale for a barrier to enter the archive is in part cost. There is an accessioning cost as well as the ongoing cost for storing material in perpetuity.

But the appraisal process itself has a cost.

In the context of the long-term preservation of digital material and where the export of AIPs is automated then appraisal is now with respect to the long-term not perpetuity. Appraisal can be linked to retention schedules and accessioning work flows can be automated. Also, the cost of storing AIPs is cheaper than if the material is not exported.

Hence the argument for the traditional approach focussed on “perpetuity” is substantially weakened. In its place archivists should be concerned with the long-term preservation of digital material, that is AIPs. As a consequence, in the future, it may be that decisions are needed about destroying legacy AIPs. Such decisions should be decided by a cost/benefit analysis and, if necessary, the GDPR (and successors).

4.7 The archive catalogue

It takes only a cursory examination to realise that an archive catalogue is substantially more information rich than other so-called catalogues (for example, a standard library catalogue). This is because the archive catalogue goes further than being a list of contents, albeit one that might be arranged by some generic scheme of classification.

The organisation, arrangement and description evident in the archive catalogue provides and demonstrates the provenance of the "record". Of itself this is an important added value intellectual contribution by archivists (Webb, 2017). "Archival practice places a premium on both collective and contextual description. The key is to explain the […] intellectual structure of the collection that may not be apparent and to provide enough contextual information for the user to understand the historical circumstances and organizational processes of the object's creation" (Gilliland-Swetland, 2000, p11).

As far as users are concerned, the catalogue also provides an information discovery mechanism. Taken together with the support for interpreting discovered information, the catalogue bolsters the integrity of the archive as a trusted resource.

4.8 Virtual signatures and sentimental documents

It was reported that some depositors believed that they had a legal duty to obtain a real signature as a subscription on paper, for example committee minutes.

Regardless of this, virtual or digital signing of documents will become universally available so that any such justification for a paper document will disappear.

Contra wise paper documents when received are often "scanned" to generate a digital image. This is then associated with material in a transaction processing system and the paper original destroyed. However it is noted that there can be original paper documents that possess unique sentimental value. For example, hand-written letters from the birth-mother being part of an adoption case. Despite there being a digital default, such paper documents should be retained.

The investigation's conclusions and recommendations are presented next in the last section of the report.

5. Conclusions and recommendations

In this section we present firstly the conclusions from the investigation and then four principal recommendations.

The investigation aims to understand how archivists can contribute to the long-term management of preserved digital material and to identify the key roles where archivists can add value. In particular Archives First should aim to influence the debate within the archives and associated information technology communities regarding the long-term management of digital material.

The report shows that archivists have the necessary theoretical framework to support the long-term preservation of digital material. If this contribution is ignored and archivists are confined to a static world of paper, then our successors will not be able to rely on vital corporate, democratic and cultural information.

The conclusions otherwise relate either to broad questions of principle or to specific aspects of preparedness that are within the archivists' scope.

It is important to maintain the collaborative momentum within Archives First to support both collective actions and actions by individual members. As John Sheridan points out, "...even in this digital age, it falls to archivists to create and sustain archives [hence they] must rapidly develop new archival practices" (The National Archives, 2017a, p6).

For example it will be crucial to identify material subject to GDPR derogations where otherwise nominal information would be deleted. Instances here include material affected by a legal hold which may be deleted when released.

Hence archivists should know what digital material is already held either within the archive or elsewhere. This may require establishing an inventory.

Archivists should also understand developments in digital preservation as well as use opportunities such as those presented by community project material to familiarise themselves with digital preservation issues, including potential ongoing costs. Helpful resources in this regard include:

The Digital Curation Centre (<http://www.dcc.ac.uk/>),
Digital Preservation Coalition (<http://dpconline.org/>),
National Digital Stewardship Alliance (<http://ndsa.org/>), and,
Open Preservation Foundation (<http://openpreservation.org/>).

Archives First is already established as a group of trusting collaborators willingly sharing experiences, practices and ideas. As such Archives First is well positioned to innovate and contribute to The National Archives' "Building the platform" programme (The National Archives, 2017b, pp9-10).

However the "elephant-in the room", the sine qua non, is how, if at all, will future computerised transaction processing systems support the export of Archival Information Packages? As illustrated by the British Library experience, this is a supplier issue. It is clearly desirable that system users, that is local authorities, should co-ordinate their requirements and act in concert.

The traditional demarcation of responsibility based on the permanent retention of material or not, is not appropriate in the context of the future digital material requiring long-term preservation. In order to reduce costs overall and to limit the exposure to risks, no-longer operational material should be exported as AIPs from processing systems. As a consequence no-longer operational material would not be migrated to successor systems. So called AIPs would need to be stored in a long-term preservation system even though this preservation may not be intended to be indefinite.

Clearly, the ability to export AIPs must become a mandatory functional requirement of local authority processing systems.

The role of information asset owner is emerging in importance. Archivists should work with information asset owners in order to manage the AIP creation and export process. This will entail ensuring not only that an information asset owner schedule is current and complete but also that retention schedules include all material required by the archive. Appendix six shows a digital continuity policy that illustrates the roles and responsibilities of information asset owners.

Archivists should be involved in all relevant system procurement exercises and together with the information asset owner, must ensure that any proposed AIP export function is adequate.

There is a pre-requisite need to work with an information asset owner to investigate in detail how for a particular system the AIP export functionality might be specified.

There is also a pre-requisite need to develop an understanding of the minimum requirements of a long-term preservation system. This system would host the AIPs.

Recommendations

There are four recommendations:

5.1 Leadership role

Archivists should adopt a leadership role in respect of issues connected with the long-term preservation of digital information. In particular they should engage with both information asset owners and technologists to become involved in system procurement. They should also identify all information which is to be retained for ten years or longer.

5.2 Skills development

Individual archivists should exploit opportunities to become familiar with digital preservation issues, terminology and practice by, for example, supporting small scale preservation projects and providing training opportunities. Innovative practice should be shared within Archives First and more broadly.

5.3 AIP export

Archives First should carry out a follow up project to investigate AIP export specification and functionality in respect of:

a) Liquidlogic Children's Social Care System (i.e. adoption cases), and,
b) modern.gov (i.e. committee minutes).

It is anticipated that the investigation here will include liaising with archivists in Scotland and will support further work aimed at specifying mandatory functional requirements to be included in future local authority system procurement exercises.

It is also anticipated that the outcome of such an investigation will be shared with other relevant consortia.

5.4 Long-term preservation of AIPs

Archives First should carry out an investigation to determine the minimum requirements of a long-term storage system for AIPs and identify available options for local authorities. It is anticipated that the outcome of such an investigation will be shared with other relevant consortia.

References

Acland, G. (1991). *Archivist – keeper, undertaker or auditor*. *Archives and Manuscripts* 19(1), pp 9-14.

Boadle, D. (2004). *Reinventing the archive in a virtual environment: Australians and the non-custodial management of electronic records*. Academic & Research Libraries 35(3), pp242-252.

Cabinet Office. (2017). *Better information for better government*. [online]. Available from: <url:https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/589946/2017-01-18_-_Better_Information_for_Better_Government.pdf>.

Duranti, L. (1996). Archives as a place. *Archives and Manuscripts* 24(2), pp 242-255.

Gilliland-Swetland, A. J. (2000). Enduring paradigm, new opportunities: the value of the archival perspective in the digital environment. Council on Library and Information Resources. Washington.

Grimshaw, J. (2017). Personal communication. [email]. British Library.

The National Archives. (2016). *Consultation on a new strategic vision for the archives sector*.

The National Archives. (2017a). *Archives unlocked: releasing the potential*.

The National Archives. (2017b). *Archives unlocked: delivering the vision*.

UK Government. (2012). *Open standards principles*. [online]. Available from <url:https://www.gov.uk/government/publications/open-standards-principles>.

UK Government. (2015). *Open standards principles*. [online]. Available from <url:https://www.gov.uk/government/publications/open-standards-principles>.

Webb, C. (2017). Personal communication. University of York.

Appendices

1. Members of the Archives First consortium

2. Project funding proposal

3. Disaster recovery versus digital preservation

4. Survey instrument

5. Local authority software applications: RM1059
    a) suppliers
    b) survey instrument

6. Digital continuity policy

Appendix one

Members of the Archives First consortium

Berkshire Record Office, West Berkshire Council; (meeting minutes, magistrates)

Dorset History Centre, Dorset County Council; (meeting minutes, adoption)

East Sussex Record Office as lead partner in The Keep, East Sussex County Council, Brighton & Hove Council, University of Sussex; (coroners, adoption).

Gloucestershire Archives, Gloucestershire County Council; (coroners, meeting minutes)

Hampshire Record Office, Hampshire County Council; (meeting minutes, adoption)

Isle of Wight Record Office, Isle of Wight Council; (meeting minutes, planning and building control)

Portsmouth History Centre, Portsmouth City Council; (meeting minutes, adoption)

Southampton Archives, Southampton City Council; (meeting minutes)

Surrey History Centre, Surrey County Council; (meeting minutes, magistrates)

West Sussex Record Office, West Sussex County Council; (coroners, planning and building control)

Wiltshire and Swindon History Centre, Wiltshire Council; (meeting minutes, planning and building control)

Appendix two

Project funding proposal

Archives First: proposed collaborative approach to digital preservation.
Application for funding from The National Archives Sustainability Fund.

1. Project overview

The world of archives is changing. Increasingly our main assets will not be produced on paper but in electronic form. As we are not primarily technologists we need to understand the contribution of archivists to the management and appraisal of electronic records to ensure that key archive sources are available for future researchers. This will in turn inform our business case for engaging in digital preservation or further developing our existing offers.

We will analyse information flow from creation to user access in both the analogue and digital world, by focusing on several key classes of records.

In order to understand the added value of archivists in the digital preservation field, we will examine the following issues through a series of pilot studies:

- What options are there in the electronic world to identify, accession, catalogue/index and provide access? What issues do these options raise?
- What standards do we need to specify?
- How do we cater for closed records, encrypted records, etc?
- How do we ensure context and provenance is preserved with digital records?
- What happens in the world of reorganisations, major governance changes (e.g. school records) and increasing local government austerity (e.g. how are privately produced, non-council records to be preserved).
- Is custody of the records essential or is the post-custodial model (where the archivist doesn't necessarily hold the digital records they are seeking to make accessible) feasible or desirable?

2. Case Studies

We propose to use the following classes of records as case studies. The following records were identified by those responding to questionnaires as the key classes to work on. At least two authorities will work on each class of records.

1. Public Records: Coroners and magistrates. Closed records. Opportunity to strengthen links with record creators and TNA colleagues.
2. Local authority: Social care (especially adoption), planning and records generated by legal/democratic services (see also section 4 below). Key record classes for making a pitch to our employers because of the legal obligation to retain long term. Opportunity to examine links to EDRMS, records management and the whole information lifecycle within our councils.
3. Private deposits: Good pilot area for learning lessons, working with records in a variety of formats, doing work on a smaller scale, benefiting from work already done within the group, examining the economics of digital preservation. Opportunity to examine potential role for others to help with digital preservation agenda.

4. Minutes and agendas: Core records of our funding bodies, and most record creators.
5. Through questionnaires we also identified areas where certain repositories have already undertaken case studies that are of particular interest to others in the area (e.g. electoral registers), so we will share lessons learnt as part of the project.

3. Background and rationale

- Within Archives First we identified getting to grips with digital preservation as our highest priority
- We see collaboration as the most effective means of tackling this area of work.
- We have undertaken two short surveys to assess knowledge levels, identify areas of learning that can be shared, and prioritise collections to use as pilot studies.
- We held a workshop led by Viv Cothey to help understand the unique selling point of the archivists' contribution to the digital preservation agenda, 12 April 2016.
- We identified this area of investigation as a gap in the market. Other regions are focusing on technical solutions.

4. Key objectives

- Identifying the key roles where archivists can add value in the digital preservation world
- Gathering quality evidence to make a strong business case for digital preservation, either individually within our own authorities, or to make a further collaborative funding bid.
- Sharing what we've learnt so far. The process itself will be a valuable learning outcome in itself, both within the Archives First grouping and more widely across the local authority sector.

5. Out of scope/limitations

We will not be focusing on a specific technological solution nor seeking to adopt prematurely such a solution, but making sure we get to grips with the wider information dimension and understand the issues in order to inform a business case, specification or future collaborative working opportunities.

6. How will the project work in practice?

To employ Cassandra Johnson from Dorset History Centre on a 2 day a week secondment basis from within the partnership. Cassandra is already well steeped in e-preservation principles. This has three advantages:

- The project does not founder through lack of capacity and has someone who can keep a good momentum going
- We don't lose six months as the project officer gets to know the topic
- Expertise is retained after the project.
- Cassandra's role will be 'back-filled' at Dorset History Centre.

To employ Viv Cothey (formerly driving the e-preservation agenda at Gloucestershire Archives, now retired but an active volunteer) as a mentor to kick-start the project and provide additional expertise as required. He has both the technical knowledge in this

specialist area and a good strategic outlook.

To consult with leading experts in the field, e.g. John Sheridan, Digital Director at The National Archives, and Jenny Bunn (archives lecturer at University College London) for advice on methodology, lessons we can learn from elsewhere, and dissemination of results.

To work through a couple of pilot areas in Gloucestershire and Dorset to work out methodology, following which the Project Officer will work with colleagues in each repository on the classes of records outlined above.

To share best practice and lessons learnt, hints and tips during the project

To hold a final Archives First workshop to evaluate lessons learnt both on digital preservation and the feasibility of collaboration across a wide geographic area and identify next steps within Archives First.

To contribute to a more sustainable approach to digital preservation learning and development for the archives sector under the auspices of The National Archives.

To share the results in a day conference at TNA part-hosted by ARA ICT section. To be further developed in conjunction with Simon Wilson and TNA and therefore excluded from the costings listed below.

7. Costings

Expenditure

- Project Officer: £ for 0.4 FTE for six months, on-costs and travel.
- Project Mentor: £ temporary register payments for time spent supporting project @ c. £ per hour (including on-costs).
- In-kind contribution of at least 5 days officer time per record office: £ (based on actual salary costs of 5 days officer time from Berkshire and Gloucestershire).
- Total: £18,550.

Income

- £ cash from Archives First (subscriptions from the participating record offices).
- £ in-kind support from contributing partners (input on their pilot classes of records; feeding in best practice, lessons learnt and contributing to the evaluation).
- We are looking for The National Archives Sustainability Fund to provide £7000 towards the cost of the salaries.

8. Project partners

- Berkshire Record Office (West Berkshire Council)
- Dorset History Centre (Dorset County Council)
- East Sussex Record Office (as lead partner in The Keep (East Sussex County

Council, Brighton & Hove Council, University of Sussex).
- Gloucestershire Archives (Gloucestershire County Council)
- Hampshire Record Office (Hampshire County Council)
- Isle of Wight Record Office (Isle of Wight Council)
- Portsmouth History Centre (Portsmouth City Council)
- Southampton Archives (Southampton City Council)
- Surrey History Centre (Surrey County Council)
- West Sussex Record Office (West Sussex County Council)
- Wiltshire Record Office (Wiltshire Council)

9. Benefits of working collaboratively

We are convinced that the only way the sector and the profession are going to be able to develop robust approaches to digital preservation is through collaboration so are keen to test the practicalities of a shared approach through this pilot project.

- Efficiencies and savings through pooling resources and expertise
- Developing skills through active participation and sharing learning in a mutually supportive way
- Maximising use of expertise within the region
- Contributing to the overall national picture by focusing efforts on the non-technological aspects.

10. What will the project deliver?

- Learning for those participating and shared expertise across the region
- Detailed evaluation of the issues identified collectively in dealing with key classes of records and record creators. Evidence and case studies for business cases to take forward digital preservation either individually or collectively to the next stage.
- Outputs for Archives First: a) report, b) case studies, c) final workshop
- Outputs for wider archival profession: d) day conference to share outcomes

11. Timescales

September 2016 – March 2017 pilot studies
Review, workshop, report and sharing findings, April – June 2017

12. Project organisation

- The Archives First Project Board members have all signed off this proposal. They will monitor project progress.
- Archives First (ie the participating offices) will agree virtually a detailed project plan and allocation of pilot work.
- Dorset and Gloucestershire County Councils will employ the project officer and project mentor and set up the detailed project plan and proposed work packages.
- West Sussex County Council will act as banker for project funds and reimburse Dorset and Gloucestershire in accordance with expenditure.

13. Appendices (not included)

1. Archives First questionnaire 1: Digital Preservation – where we are now.
2. Invite to Archives First workshop, 12 April arising from questionnaire 1.

3. Archives First questionnaire 2: Record classes and areas of existing expertise. The responses have informed the choice of case studies proposed in this project.
4. Role profile of project officer

Disaster recovery versus digital preservation

Disaster recovery planning includes (but is not restricted to) strategies for data protection. Such strategies aim to ensure that as much data as possible remains available after a disaster. Common approaches for data protection involve data backup coupled with (multiple) off-site backup storage. Data restoration is achievable up to the time of the most recent backup. The goal of disaster recovery is to be able to re-establish critical business operations as quickly as possible with the minimum of data loss. The viability of disaster recovery planning includes regular data restoration testing.

Digital preservation also includes strategies for data protection. However it is not concerned with operational data. Therefore there is no need to plan a restoration as described above. The principle requirement of a digital preservation data protection strategy is zero data loss. Although there is a potential requirement to be able to access any of the data, it is probable that a large proportion of the data will not be accessed for decades (if at all). The viability of a digital preservation data protection plan includes regular fixity testing. (Fixity is a computing procedure which examines the stability or absence of change of a computer file over time.) Note that a data protection strategy for digital preservation will also require multiple off-site data backups.

Survey instrument

Archives First digital preservation: detailed survey

Introduction

This survey aims to build a comprehensive picture of the current flow of information throughout its lifecycle. We hope to be able to identify commonalities which can inform collaborative action.

The questions are divided into four sections:

- Section A - to be answered by all participants as far as possible
- Section B - to be answered with reference to the first record type you have been allocated
- Section C - to be answered with reference to the second record type you have been allocated
- Section D – points for discussion if not covered in the course of the conversation

Survey

A. Systems for the management of current / semi-current information
Please indicate where the systems have been developed in-house rather than procured commercially; or if no electronic records management system is in use.

The depositing body is taken to mean the organisation from which you seek to acquire records. If you have information about more than one depositing body please include it clearly identified.

1. What system(s) does the depositing body use for the management of information relating to committee meeting papers? e.g. agenda and minutes?

2. What system(s) does the depositing body use for the management of information relating to adult social care?

3. What system(s) does the depositing body use for the management of information relating to children's social care, including adoption records?

4. What system(s) does the depositing body use for the management of information relating to planning applications?

5. What system(s) do your local Magistrates Courts use for the management of information relating to court proceedings?

6. What system(s) does your local Coroner's Office use for the management of inquest files?

7. Does your parent organisation have a digital continuity policy? Were

archivists involved in its production?

B. Record type 1

Please specify record type:

1. Are these records being created and managed electronically?

   Yes No

   Partly (please provide detail)

2. Are these records suitable for access by the general public? E.g. no Data Protection issues

   Yes (go to Q 2.1) No (go to Q 3)

   2.1 Does the management system facilitate online publishing of the records?

   2.2 How long does this information remain available online?

3. Where is the data managed by the system (as identified in part A) held? E.g on council owned servers / externally hosted

4. Do you have any information about the re-procurement cycle / future plans for the system in which these records are created and managed? Please detail

5. Does the system in which these records are created and managed allow the export the export of non-operational data? E.g. data which is no longer in current use.

6. Is the data encrypted whilst at rest in the current system? (rather than during transit between systems)

7. Is there a documented exit strategy in place? E.g. to transfer data to a new system / the system provider goes bust

8. Are these records currently regularly transferred to a records management team?

   Yes – paper No – paper
   Yes – digital No – digital

9. Has the depositing body/system provider made any plans for the permanent preservation of any of their electronic records?

10. Are any of the records in this class currently regularly transferred to the archive service? Where paper based systems operate in conjunction with

electronic please detail these.
team?

Yes – paper (go to Q 10.1) No – paper (go to Q 11)
Yes – digital (go to Q 10.1) No – digital (go to Q 11)

10.1 Please detail any metadata that is provided with the transferred

10.2 What is the retention trigger for transfer to the archives?

10.3 What provision is there for storage of the records and related metadata upon transfer to the archives? (Where/how files and metadata are stored, who manages this etc.)

10.4 What level of cataloguing is usually applied to these records? E.g. box-listing/full item level cataloguing

10.5 How is access provided to the catalogue information?

10.6 How is access provided to digital records, if at all?

10.7 What are the barriers to providing access to digital records?

11. What are the barriers to accessionaing these records in a digital format? E.g. technology, resources etc.

Please attach examples of metadata generated at any relevant point during this process e.g. originating system generated / acquired on transfer / catalogue records.

C. Record type 2

Please specify record type:

1. Are these records being created and managed electronically?

Yes No

Partly (please provide detail)

2. Are these records suitable for access by the general public? E.g. no Data Protection issues

Yes (go to Q 2.1) No (go to Q 3)

2.1 Does the management system facilitate online publishing of the records?

2.2 How long does this information remain available online?

3. Where is the data managed by the system (as identified in part A) held? E.g on council owned servers / externally hosted

4. Do you have any information about the re-procurement cycle / future plans for the system in which these records are created and managed? Please detail

5. Does the system in which these records are created and managed allow the export the export of non-operational data? E.g. data which is no longer in current use.

6. Is the data encrypted whilst at rest in the current system? (rather than during transit between systems)

7. Is there a documented exit strategy in place? E.g. to transfer data to a new system / the system provider goes bust

8. Are these records currently regularly transferred to a records management team?

Yes – paper	No – paper
Yes – digital	No – digital

9. Has the depositing body/system provider made any plans for the permanent preservation of any of their electronic records?

10. Are any of the records in this class currently regularly transferred to the archive service? Where paper based systems operate in conjunction with electronic please detail these.
team?

Yes – paper (go to Q 10.1)	No – paper (go to Q 11)
Yes – digital (go to Q 10.1)	No – digital (go to Q 11)

10.1 Please detail any metadata that is provided with the transferred

10.2 What is the retention trigger for transfer to the archives?

10.3 What provision is there for storage of the records and related metadata upon transfer to the archives? (Where/how files and metadata are stored, who manages this etc.)

10.4 What level of cataloguing is usually applied to these records? E.g. box-listing/full item level cataloguing

10.5 How is access provided to the catalogue information?

10.6 How is access provided to digital records, if at all?

10.7 What are the barriers to providing access to digital records?

11. What are the barriers to accessionaing these records in a digital format?

E.g. technology, resources etc.

Please attach examples of metadata generated at any relevant point during this process e.g. originating system generated / acquired on transfer / catalogue records.

D. Discussion points

1. When should (if at all) the archivist intervene in the preservation of records requiring long-term (but not permanent) retention? How do we define “long-term”?

2. When / how does the role of RM/IT interact with the archives?

3. When should the archive take custody of records requiring permanent preservation? E. g in the case of the 20 year rule – would 20 years be too late?

4. (When) should archives catalogue records not transferred to the care of the archives?

Local authority software applications: RM1059: suppliers

See: Crown Commercial Services: Local authority software applications <https://ccs-agreements.cabinetoffice.gov.uk/contracts/rm1059>

(see lots 3 and 6)

Agile Applications Ltd

Arcus Global Ltd

Azeus UK Ltd

Bramble Hub Ltd

Capita Business Services Ltd

CareWorks Ltd

Civica UK Ltd

Corelogic Ltd

Def Software Ltd

Idox plc

Liquidlogic Ltd

OLM Systems Ltd

Open Sky Data Systems

Oxford Computer Consultants Ltd

Quickheart Ltd

System Associates Ltd

Tascomi Ltd

Tribal Education Ltd

Local authority software applications: RM1059: survey instrument

Archives First

Background: preserving information in local government

"Archives First" is a collaborative project involving eleven English local government authorities and is sponsored by The National Archives.

Local authority Record Offices (or their equivalent) have been responsible for ensuring the preservation of selected paper based records in order to capture the corporate memory of the organisation and meet legislative requirements. However local government is in the process of moving from paper to "digital working". The objective of the Archives First project is to investigate future arrangements for preserving digital records.

The purpose of this questionnaire is to survey the relevant capabilities of local authority software applications provided by suppliers described in Lot 3 (Environmental Planning Building Control Trading Standards and Licencing systems) and Lot 6 (Social Care) of the Crown Commercial Service agreement.

In the event that you have any questions or require clarification then please contact:

Cassandra Pickavance, Archivist / Project Officer
c.m.pickavance@dorsetcc.gov.uk | 01305 228937

Survey

We would be most grateful if you would provide answers to the following:

1. Supplier name

2. Your contact information
   Name:
   Email address:
   Telephone:

3. System/Product names and application area e.g. environment, adult social care. It would be most helpful if you could also let us know the number of customers each system is supplied to.

4. Please answer in respect of each system

   4.1 System life expectancy.

4.1.1 Do you have a published “end of life”?
4.1.2 If not then for how long do you currently offer support?

4.2 Record life expectancy
4.2.1 Is the system designed to retain records for up to 15 years?
4.2.2 Can the system retain records in excess of 50 years?

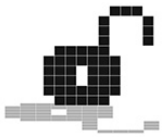
4.3 Export
4.3.1 How does the system support the export of records both bulk and individual?
4.3.2 What format standards are available e.g. text, png?

4.4 Long-term storage
4.4.1 Does the system already support the long-term storing (multiple decades) of non-operational records? If not then do you have any plans to provide for long-term retention.

Please provide details.

Thank you.

Digital continuity policy



information
management & security

Gloucestershire
COUNTY COUNCIL

Gloucestershire County Council
Digital Continuity Policy

1. Policy Statement and Purpose

Digital continuity is the ability to use your electronic information in the way you need for as long as you need. Losing digital continuity means you are not able to **find**, **open**, **work with**, **understand** or **trust** your information. The loss of usability is an information loss as significant and potentially damaging as any other. Loss of digital continuity is an information risk that is increased by technical, organisational, or business change. These risks can increase over time if not managed from the outset.

An example of where information becomes unreadable due to technological obsolescence is where it was created using a now superseded version of software or is stored on outdated media such as floppy disks. Many information assets are required to last longer than the technology on which they are created or currently stored (software and hardware).

The purpose of this policy and related guidance is to produce a consistent approach to protect the Council's information assets and reduce the risk of unintentional information loss.

2. Scope

This policy applies to the management of digital information throughout the Council. All those responsible for managing the Council's information assets and/or managing the introduction of new systems development or implementation must adhere to this policy.

3. Risk Management

Potential risks include being unable to find, open, read, work with, understand or trust your information leading to legal, reputational or financial consequences or inability to offer aspects of a service.

4. Requirements for digital continuity

4.1 Information asset owners must ensure the digital continuity of the information for which they are responsible. They need to be aware of what technology their information assets and operational systems rely upon.

4.2 Digital continuity must be taken into account whenever

- procuring new systems
- managing information migration between systems
- decommissioning systems.

4.3 Digital continuity risks must be managed using the corporate risk framework.

4.4 Where information assets need to be maintained for longer than the expected life of the operational system there must be an exit strategy for digital continuity to safeguard information assets when the system is decommissioned.

4.5 A digital information storage system should be created to retain legacy digital information non-operationally where this is more economic than leaving such information in operational systems.

4.6 Legacy digital information must not be encrypted but stored securely.

4.7 Scheduled information asset destruction (as per retention schedules) must be regularly and securely undertaken to ensure compliance with statutory obligations and to reduce storage costs.

5. Roles and Responsibilities

5.1 Gloucestershire Archives is responsible for developing professional standards for digital continuity and associated guidance, and for ensuring that records identified for permanent preservation are preserved as appropriate.

5.2 Senior managers are responsible for ensuring information assets have an appropriate nominated owner, and that this policy is implemented within their areas.

5.3 Information Asset Owners are responsible for ensuring the digital continuity of their information assets as set out in section 4.1-4.4 and 4.6-4.7 above.

5.4 Archives, Information Management and ICT colleagues are responsible for ensuring digital continuity issues are considered and included in relevant strategies and projects, and collaborating to facilitate good management of information throughout its lifecycle. They will also collaborate to address section 4.5 above.

6. References

This policy and other related information management policies can be found at http://www.gloucestershire.gov.uk/council-and-democracy/strategies-plans-policies/information-management-and-security-policies/

Digital preservation policy can be found at http://www.gloucestershire.gov.uk/archives/policies

Digital continuity guidance for information asset owners can be found at Appendix 1 below.

Other related guidance includes:

Business continuity planning at https://staffnet.gloucestershire.gov.uk/public-facing-departments/community-services/business-continuity-management/

Records retention schedules at
https://staffnet.gloucestershire.gov.uk/media/3431/retention-schedule-v13.pdf

7. Review and Revision

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 3 years.

Document Control

Authors:	Viv Cothey, E-preservation archivist, and Heather Forbes, Head of Archives Service
Owner:	Jane Burns (Chief Information Officer)
Approval Body	Information Board
Date Approved	14 March 2017
Document Number:	V1.2

Revision History Date of next revision: March 2020

Revision date	Summary of Changes
Jan 2012	V0.1 adjusted following consultation with information management/security, ICT, emergency management and sample information asset owners and administrators.
Mar 2012	V1.0 approved by Information Board
Nov 2012	V1.1 Non-encryption requirement added, requirements in section 4 clarified, links updated. Link to digital preservation policy added.
Mar 2017	V1.2 Links updated and section 5. Responsibilities added. Reviewed by current Information Board and Appendix 1: Guidance for Information Asset Owners added.

Appendix 1: Guidance for Information Asset Owners
Information Asset Owners need to ensure information for which they are responsible is usable for the entire length of its retention period. Many information assets are required to last longer than the technology on which they are created or currently stored (software and hardware).

Current systems
As part of your annual review of information assets:

- Check how long you need to retain the information in the current system (i.e. operational data), and when it can be deleted or transferred to Gloucestershire Archives.
- Securely dispose of information no longer required. First make sure that it has reached the end of its retention period (and is not marked Review or Transfer to Archives in the corporate retention schedule).

- Review growth rates and identify opportunities for savings and efficiencies – e.g. moving to cheaper storage. Does all your data need to be on level 1 storage (i.e. immediately available and backed up daily) rather than cheaper level 2 storage?
- Be aware what technology your information assets rely on. E.g. what software and operating system are used and when these are due to fall out of support, how information is recovered in the event of a disaster, and what technical tools are available for exporting data at the end of system's life or your contract with the supplier.

End of software life or contract

- Have a migration strategy in place which covers operational and non-current data. E.g. how will you export your data, and in what format? E.g. Don't leave behind information required for any future purposes in a legacy system that is no longer supported or copy onto a memory stick.
- Non-operational digital information (e.g. closed case files stored outside the operational system) must not be encrypted but must be stored securely.

Commissioning new systems

- You must take digital continuity (and end of life migration strategy) into account when procuring a new system.
- Specify who owns the data.
- Specify the ability to extract your data in a usable form at no cost/low cost.
- Specify the ability to delete your data (both individual records and en masse) when it comes to the end of its retention period.
- Arrange an ESCROW[1] agreement where appropriate.
- Include information as part of your change management policies and procedures. Test business critical information before and after change to ensure you can still use it as you need to.

Further Advice.

Gloucestershire Archives staff have been developing expertise in dealing with electronic records that need to be retained long term and/or in perpetuity, using the OAIS model developed for the space industry (ISO 14721:2012). They are currently working with ICT colleagues to develop a 'trusted digital store' for records required for long term preservation. And with sample information asset owners to develop guidance on extracting data from live systems for long term preservation purposes. Further guidance to follow. Please contact archives@gloucestershire.gov.uk for advice in the meantime.

1An *escrow agreement* is an arrangement where one party deposits an asset (e.g. computer code) with a third person (called an *escrow* agent), who, in turn, makes a delivery to another party if and when the specified conditions of the contract are met (e.g. ICT supplier ceases trading).