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example of where information becomes unreadable due to technological obsolescence is where it was created using a now superseded version of software or is stored on outdated media such as floppy disks.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 considered 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 over the long term but stored securely. If encryption keys are lost, it will be impossible to access the information being preserved. If encryption is deemed essential for longer term storage of certain information, then documented regular checks of encryption keys will be necessary.

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 (IAOs) 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. You can find out more about IAOs on the Information asset owners help and guidance pages.

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 and data management policies can be found on the Information Management and security policies page.

The digital preservation policy

Gloucestershire County Council's digital strategy

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

Other related guidance includes:

Business continuity planning

Records retention schedules

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:	Claire Collins, Digital Archivist, Viv Cothey, Digital Archivist, and Heather Forbes, Head of Archives Service
Owner:	Rob Ayliffe (Senior Information Risk Owner)
Approval Body	Information Board
Date Approved	15 September 2020 [v1.3]
Document Number:	V1.4

Revision History   Date of next revision: 2023

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.
Aug 2020	V1.3 Links updated. Requirements for digital continuity at 4.6 updated. Link to IAO advice added at 5.3. Owner updated. Link to Digital Strategy added. Appendix 1 further advice updated.
Nov 2022	V1.4 Accessibility issues addressed and SIRO updated.

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 or a disorderly exit (such as the sudden collapse of your supplier or storage provider), 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 escrow agreements (or equivalent) as appropriate. An *escrow agreement* is an arrangement where one party deposits an asset (e.g. computer code or data) 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).
- 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 developed expertise in dealing with electronic records that need to be retained long term and/or in perpetuity, using the OAIS model for digital preservation (ISO 14721:2012). Please contact archives@gloucestershire.gov.uk for further advice.