Gloucestershire County Council
Scanning Policy

1. Policy statement and Purpose

Gloucestershire County Council is transforming the way it does business, moving towards increased digital ways of working, both internally and in the provision of digital services to its customers.

Scanning is the process of digitising paper-based information for business use and storage as electronic/digital records. The scanning process must safeguard the authenticity, reliability, integrity and availability of information, so that the information remains useable and of value to the council. The Council also has a responsibility under the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA) to process personal data in a manner that ensures appropriate security of the data. All staff are responsible for protecting the information the council collects and holds, identifying and managing any associated risk.

The purpose of this policy is to ensure that all scanning processes undertaken within the council:

- Protect the authenticity, reliability, integrity and availability of the council's information including personal data;
- Comply with the requirements set by related legislation and standards (see Appendix 1)
- Provide legal admissibility where necessary;
- Represents best value for money, taking into account both short and longer-term impacts of scanning information.
- Manages risk proactively

2.0. Scope

This policy covers all scanning processes undertaken within the council where the original paper copy will be destroyed including:

- established day-to-day scanning activities
- Ad-hoc scanning activity
- Discrete scanning projects

The policy applies to all information being scanned and all members of staff participating in the scanning process including the authorisation of the process**.**

3.0. Requirements for Scanning

3.1. Business Case

All scanning activity must be warranted. Scanning projects should only be undertaken once a strong business case has been developed and approved at an appropriate level. All relevant stakeholders must be consulted to ensure that all their requirements are taken into account. Those consulted will include stakeholders in the Information Management Service. Stakeholders' comments and/or requirements must be set out in the business case.

Each project should be assessed separately based upon its individual purpose and the necessity of the scanning activity. The following should be key considerations:

Cost .v. Benefit

- What is the cost of the scanning process? *Take into account the cost of all resources, including time, people and equipment: e.g. how much time will need to be spent removing staples and paperclips?*
- What is the cost of storing the electronic information over its whole lifecycle? Is it cheaper or more expensive than storing paper records in the Records Centre? *Contact the Records Centre for storage costs.*
- Is there available equipment that can scan to the requirements described in this policy? *The digital images created by the scanning process need to be in a reusable format to ensure that they support the delivery of relevant council activities.*
- How many people need access to the information and what type of access is required? *Enabling information to be accessed by multiple individuals, as part of a distributed audience at the same time enables collaborative working.*
- How frequently is the information used? *If the information is in constant use, it may be easier to refer to a digital copy, rather than the paper original.*
- Which activities does the information support? Digitising information and pulling it together can support the work of *investigations, and inquiries.*

Suitability of records/information for scanning

- What condition are the paper originals in? *Fragile or oversized paper records may not be suitable for scanning.*
- Will the information's readability be enhanced by scanning? *Poor quality paper records may require considerable enhancement to produce a good digital image.*
- Will you be scanning material that is only currently available in paper form? *Ensure that there isn't already a digital copy of the information. Don't re-scan print-outs of information that was created electronically.*

- How long does the information need to be kept for? *Information with a very short retention period may not be worth scanning. Records that have reached the end of their required retention periods should not be scanned. The Council bears the costs of storing, backing up and migrating irrelevant scanned data. The Council's Records Retention and Disposal Schedule lists the length of time records (whether in paper or scanned form) need to be kept.*

Ongoing Management of the electronic information

- Where the digitised information will be stored? *The information needs to be saved securely to an appropriate location on a GCC system or network drive.*
- How robust are the systems for storing the information? *Consider the information security arrangements in place and whether they provide an adequate level of protection for the information.*
- Who will be responsible for managing the digitised information as part of business as usual? *Roles and responsibilities for managing the information must be clearly defined and understood.*
- What measures will be in place to enable long-term accessibility of digitised information? *Some information may need to be retained for several years. Plans need to be in place to ensure ongoing software and hardware availability, as part of managing ongoing technological innovation and changing ICT practices within the council.*
- What processes will be in place for disposal of information? *Information needs to be disposed of (i.e. either destroyed or transferred to Archives) at the end of its retention period. Systems need to have retention and disposal functionality to ensure appropriate action takes place at the right time.*

3.2. Legal Admissibility

The legal admissibility of any document must be taken into account before scanning activity begins. There is no definitive legislation regarding legal admissibility of scanned documents over paper originals but electronic copies will be accepted as best evidence provided they are of a sufficient quality to ensure readability and are proven to be identical to the originally created document.

- Some high risk documents, such as documents under seal and deeds, will need to be retained as paper originals. More generally, if the original paper record still exists, this will generally be preferred over a scanned copy (the 'best evidence rule').

- BSI BIP 0008-1:2014 is the British standard on legal admissibility and evidential weight of information stored electronically. Any electronic document that could be relied on in court must have been scanned in accordance with this standard. Complying with this standard ensures the council's electronic records are captured, stored and managed in a way to maximise evidential weight and demonstrates the contents of the electronic documents haven't changed.[1]

[1] A copy of the standard and an associated compliance workbook are available from the Information Management Service.

- Documented and secure processes must be in place to help demonstrate the authenticity of the scanned copies and evidence that they have not been tampered with.

When legal admissibility is likely to be an issue, it is recommended that project managers consult with Legal Services.

3.3. Confidentiality, security, access

- Scanning should take place in a secure environment, appropriate to the level of sensitivity and confidentiality of the information;
- Scanning of personal data including special category (sensitive) data must only be undertaken by persons authorised to do so, e.g. persons who have permission to view the information as part of their day-to-day role.
- Information Asset Owners must provide permissions, documented in advance, for individuals employed to carry out discrete scanning projects to view the information.

3.4. Technical requirements

- Technical requirements will vary according to the purpose and business needs of individual projects. These must be discussed with the ICT as part of the normal ICT project management framework.
- Business analysis within individual projects will identify appropriate file formats; resolution and possible compression, such as lossless[2]; suitable hardware, server space, backup and recovery arrangements; ensuring sufficient bandwidth; and integration with existing databases if required. The analysis will also determine the most appropriate scanning methodology (e.g. back-scanning[3], scan on demand[4], day-forward scanning[5]) and whether scanning should be undertaken in-house or out-sourced.

When scanning is undertaken in-house, existing software will be used where feasible. Multi-Functional Devices (MFDs) are only suitable for ad hoc small-scale scanning

3.5. Quality Control

- Before starting scanning projects and/or scanning in bulk, always scan a test document and compare the test scan with the original paper document to assess quality and identify any issues and required solutions.

[2] Lossless data compression is a class of data compression algorithms that allows the exact original data to be reconstructed from the compressed data.
[3] Typically the scanning of old paper files undertaken as a large-scale, one-off exercise.
[4] Scanning undertaken on an on-going basis as required
[5] Scanning all material from a specific date onwards.

- Quality checks of all scanned images must be carried out as soon as the scanning has taken place. Required checks include ensuring:
  - ✓ Every piece of a paper document has been scanned, including blank pages, double-sided documents and post-it notes.
  - ✓ No changes have been made to the document within the scanning process: the electronic information is an exact representation of the paper original.
  - ✓ The electronic record is readable.
- Do not destroy the original paper record until the quality and authenticity of the electronic record has been signed off.

3.6. Indexing and Auditing

- Scanned records should be given a meaningful title and saved on an appropriate council network drive or system.
- Specific sets of metadata, such as reference number, name/title of document, date of document, time and date of scanning and owning service area must be attached to all scanned documents. This metadata facilitates retrieval, filing and decisions about retention.
- Maintain audit trails of scanning activity within projects, recording batch numbers; dates of scanning; and if appropriate, how many blank pages in the original record have been dealt with.
- Files sent to a third party for scanning must be transmitted securely and information must be appropriately managed and accounted for at all times. If personal data is involved, the contract with the third party must ensure the records are scanned and stored in accordance with GDPR and the DPA 2018. The data transfer list must be sufficiently detailed to be able to retrieve files if needed for a statutory subject access request for instance, to ensure that no records have been lost in transit, and to check invoices for scanning work completed.

3.7. Retention of information

- Original paper documents should be retained until sufficient quality checks have been carried out on the image and the electronic copy has been correctly indexed and is stored securely.
- Unless the original paper records are marked in the retention schedule as “transfer to Gloucestershire Archives”, once the quality checks have been confirmed, the paper original should be securely destroyed, with a record of the destruction maintained.
- From the outset, consider how the electronic records will be disposed of at the end of their retention period. Personal data kept too long could lead to fines under GDPR and the DPA 2018, and all material held beyond its retention date remains accessible under the Freedom of Information Act.
- For records ear-marked for transfer to archives, consult Gloucestershire Archives before destroying paper originals to ensure that the long term

preservation and access requirements to the scanned records are sufficiently robust and sustainable.

3.8. Digital continuity

- If scanned records have a long retention period, it is likely that they will be migrated from one system to another at least once during their lifecycle. The potential costs and risks of migration should be considered in the original business case. At upgrade it may be appropriate to archive some scanned material to a preservation environment, rather than migrating it all to the new live system.
- Scanned copies are susceptible to corruption and loss, which can be unpredictable, sudden and total. Continued access, a means of demonstrating authenticity (tested periodically), backup and recovery procedures are therefore important.
- Records scanned for long-term preservation must not be stored on removable media e.g. USBs, CDs or DVDs.
- Digital continuity guidance can be found at http://www.gloucestershire.gov.uk/media/6625/digital_continuity_policy_2012__v1-1-57807.pdf

4.0. Roles and Responsibilities

- **Staff** – all staff are responsible for managing and protecting the council's information; engaging with and following this policy, ensuring that information is scanned in line with the guidance provided.
- **Project Managers** – are responsible for adhering to this policy throughout the delivery of their project.
- **Project Sponsors** – are responsible for policy compliance.
- **Information Asset Owners** – are responsible for undertaking information risk assessments and ensuring that any scanning activity does not place the information at unnecessary risk at any stage during its lifecycle. This involves agreeing access permissions; and regularly reviewing compliance with standards for authenticity and evidential weight and maintaining evidence of compliance.
- **Information Management Service** – is responsible for developing policies and guidance on managing information throughout the scanning process; providing support to staff on the handling, storage and disposal of information.
- **ICT** – is responsible for providing advice and support regarding technical requirements for scanned images; equipment and software.
- **Gloucestershire Archives** – is responsible for providing guidance to staff on which records need to be retained in for long-term or permanent preservation; developing policies and guidance on digital continuity.
- **Third Party Scanning Operators** – are responsible for complying with the terms set out in any contract with the Council and this policy.

5.0. References

- The Digital Continuity policy.
- The Digital Preservation policy.
- The Information and Data Management Strategy

6.0. Review and Revision

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

Appendix 1. Legislation and Standards

The following legislation and standards have informed this policy.

- General Data Protection Regulations and the Data Protection Act, 2018
- Civil Evidence Act, 1995
- Freedom of Information Act, 2000
- BS 10008 Electronic Information. Correct Storage of Digital Information
- BSI BIP 0008-1:2014: Evidential Weight and Legal Admissibility of Information Stored Electronically. Code of Practice for the Implementation of BS 10008
- ISO/TR 15801:2009 Document Management – Information stored electronically – Recommendations for trustworthiness and reliability.
- BS ISO 15489-1 and 2: 2001. Information and Documentation – Records Management: General and Guidelines.

Document Control

Owner:	Jane Burns, Chief Information Officer
Author:	Heather Forbes, Head of Archives
Last Reviewer:	Michelle Conway, Information & Records Team Manager
Approval Body	Information Board
Date Approved	28 November 2012
Next review date:	July 2021
Document Number:	V2-0

Version	Version date	Summary of Changes
0-1	2009, Jun	Circulated to Information Management Group
0-2	2010, Dec	Significant re-write circulated to IMG, ICT and colleagues undertaking scanning: policy statement and further information on long term implications and costings
0-3	2011, Mar	Recast with focus on business requirements

1-0	2012, Nov	BS10008 and digital continuity and preservation policies added; information asset owners and client liaison arrangements updated; reformatted.
1-1	December 2016	Updated links to new ICT pages on staffnet
2-0	July 2019	Significant re-write; removed references to BSI BIP 0008-2:2008, now superseded by BSI BIP 0008-1:2014, with additional references made to the new standard; references made to GDPR and DPA 2018, which have superseded DPA 1998; additional roles and responsibilities added; updated hyperlinks due to new IMS pages on staffnet