Corporate Scanning Policy

1 Version History details and author

1.0	Nov 2016	Completed for Distribution	David Jenkins
2.0	09/01/2017	Approved by Information Governance Group.	David Jenkins
3.0	05/02/2018	Reviewed by Information Governance Group. No changes.	Mark Smith
4.0	04/03/2019	Reviewed by Information Governance Group. Specifics of how scanned images are stored have been removed.	Mark Smith
4.1	28/05/2019	Alterations to facilitate practical implementation by Derbyshire Business Centre, including removal of references to the (defunct) Corporate Scanning Procedures.	Mark Smith
4.2	19/06/2019	Experimental version, incorporating minimum requirements for scanning outside the BS 10008 framework. Minor amendments following feedback from Tom Mainprize.	Mark Smith
5.0	08/10/2019	Clarification in s5 that a formal proposal may not be a requirement; Minor re-wording of role descriptions; Space in table for reviewer/owner, and link to local scanning guidance; Other minor edits: typos, table formatting.	Mark Smith
6.0	03/11/2020	Approved by Information Governance Group. No changes.	Mark Smith
7.0	02/11/2021	Approved by Information Governance Group. No changes.	Mark Smith
8.0	06/12/2022	Approved by Information Governance Group. Appendix removed for accessibility.	Mark Smith
9.0	09/01/2024	Approved by Information Governance Group. No changes.	Mark Smith

This document has been prepared using the following ISO 27001:2022 standard controls as reference:

ISO Control A.5.10 - Handling of assets

ISO Control A.5.12 - Classification of information

ISO Control A.5.13 - Labelling of information

ISO Control A.5.31 - Identification of applicable legislation and contractual requirements

ISO Control A.5.36 - Compliance with security policies and standards

ISO Control A.6.3 - Information security awareness, education and training

ISO Control A.7.10 - Disposal of Media

2 Introduction

Derbyshire County Council is committed to the adoption of electronic working methods. These include the creation of scanned versions of original paper documents. With proper management of the process, it is possible to take a scan from paper and choose to treat the electronic scan as the record, allowing the paper original to be destroyed. To do this, the resultant electronic image must possess the qualities of a record identified in BS 15489 i.e. authenticity, reliability, integrity and useability.

3 Scope

This policy applies to all scanning operations carried out with the aim of creating an electronic version to be treated as the record and managed according to the Corporate Records Management Policy. These operations take two forms:

- High-volume scanning projects, undertaken within the framework of the BS 10008 standard. The procedures in place at Derbyshire Business Centre have been designed to meet this standard, and the facilities there are capable of accommodating projects such as the retrospective scanning of a large body of paper records ("back-scanning"). BS 10008-compliant scanning procedures are also in place in other settings, such as the Shared Services Centre, where back-scanning of human resources files takes place.
- Local scanning operations outside the BS 10008 framework. Scanning is routinely performed on desktop scanners and multi-function devices (MFDs) by staff in local business areas.

The information which may be scanned in accordance with this policy includes (but is not limited to) Human Resources, Finance, Health and Safety, and Social Care.

Documents which fulfil no evidential purpose are outside the scope of this policy and may freely be scanned as information without reference to it, but with due regard for information security and intellectual property law.

4 Applicable standards

Derbyshire County Council's information management framework is outlined within our ISO27001 certification Information Security Management System. Rules on the retention and disposal of information can be found in the council's records retention schedules as identified in the Records Disposal Policy and Procedures. The council's rules on information security are defined under its Information Security Policy framework including information classification, cryptographic controls and back-up and restore procedures. These rules should be followed throughout any scanning process.

The BS 10008 standard is designed to maximise the evidential weight and legal admissibility of electronic information.

5 Authenticity and Legal Admissibility

All scanning will aim to create a digital version which is as close to the paper original as possible. In defence of authenticity, creators of electronic records drawn from paper originals should take steps to minimise risk of any loss in evidential value. A user of the new electronic version should be no less able to find out who created the record, who has had access to it, and whether or when it has been modified.

Evidential value is never more important than when records are produced in court. The Civil Evidence Act 1995 permits records of local authorities to be admitted into evidence in civil

proceedings if offered together with certification that these are local authority records. The Act also states that copy documents may be admitted, whether or not the original has been destroyed. However, the copy should be "authenticated in such manner as the court may approve". This wording means it is up to the courts to determine the best way to verify copies; in the case of digital copies, there is no significant body of case law to offer clarification.

Rules for criminal proceedings acknowledge similar principles. The Police and Criminal Evidence Act 1984 permits admission of copies and also mentions certification. A digitally scanned image must be accompanied by a certificate issued by the person responsible for the scanning system, confirming that the equipment used was operating correctly at the time the copy was taken, and that any defects were too minor to affect the accuracy of the record.

Scanning in accordance with the BS 10008 standard generates a substantial audit trail which identifies the original documents, the personnel responsible for carrying out the work, the personnel responsible for quality-checking and the dates/times on which scanning was done and the originals destroyed. It also requires the continuous maintenance of logs of any defects in the operation of the hardware. High-volume scanning projects should always be performed in accordance with the BS 10008 standard.

6 Procedural requirements

Scanning in compliance with BS 10008 must be carried out in controlled conditions in a regulated and secure environment, such as Derbyshire Business Centre, by staff who have been given appropriate training which is regularly refreshed. In order to ensure the integrity of the scanned images, procedures should require that checks are made to minimise the risk of information loss at any point in the process, from transfer to eventual scanning. The procedures should result in the creation of an audit trail as identified in the Code of Practice for the implementation of the standard. This audit trail should comprise an unalterable record which identifies the nature of the original documents, the personnel responsible for carrying out the work, the personnel responsible for quality-checking and the dates/times on which scanning was done and originals destroyed. BS 10008 also requires the continuous maintenance of logs of any defects in the operation of the hardware.

The initiator of any high-volume scanning project is responsible for the production of a project proposal, and risk assessment relating to the destruction of hard copy originals, addressing specific issues of authenticity and integrity of information.

Where scanning operations are carried out outside the BS 10008 framework, e.g. scanning operations on multi-function devices (MFDs), a formal proposal is not required but may still prove useful. In all cases, scanner operators should be assisted by formal procedural guidance. The procedure document should:

- have a clearly defined scope and an identified owner;
- be regularly reviewed;
- identify the system(s) in which the scans will be maintained as records;
- require a regular assessment of how well the procedure is being followed;
- allow for destruction of hard copy originals subject to the production of a risk assessment (e.g. using the form in Appendix 1).

Each scanning risk assessment should have a clearly defined scope and an identified owner, and be subject to regular review. It should address issues pertaining to a defined body of records which share common characteristics. The definition should be narrow enough to give an accurate account of similar risks, but broad enough to avoid duplication

and maximise efficiency. Each risk assessment should cross-refer to the relevant Information Asset Register, and should identify any records which must continue to be maintained in hard copy for specified legal or business reasons (e.g. personal documents which are the property of service users, documents providing legal certification of an event, documents authenticated by an attachment such as a seal, documents of which the authenticity is likely to be challenged).

Risk assessments, assessments of compliance with BS 10008 and assessments of compliance with a scanning procedure should be retained for at least as long as the scanned records to which they relate.

7 Consultation with key stakeholders

As part of any high-volume scanning project appropriate consultations will be made to ensure the requirements of stakeholders are taken into account. These consultations will include internal stakeholders in Legal Services, Information Security, Records Management, and Audit Services.

Each project should begin with a scanning proposal and risk assessment (see Appendix 1). Information Governance Group representatives from Legal Services, Information Security, Records Management and Audit Services shall be invited to review each proposal and risk assessment. Additional consultations may be carried out depending on the type of scanning project (e.g. HRMC may be contacted if scanning financial records).

Stakeholder consultations are not required for local scanning operations outside the BS 10008 framework, but the applicable procedures and risk assessments should be owned by appropriate senior managers and regularly reviewed.

8 Roles and Responsibilities

Chair of the Information Governance Group will act as a high level sponsor for scanning and arrange approval of all appropriate policies and procedures.
Corporate Records Manager will manage the development of the policy and procedural framework for scanning.
Derbyshire Business Centre Manager will manage the practical application of the content of this policy at the Derbyshire Business Centre, including continued compliance with BS 10008.
ICT Services will manage development of the software associated with the storage of scanned images and provision of resources to support the scanning framework.
Information Governance Group representatives: will respond to scanning proposals to establish their views on whether a proposal should proceed.
Senior Managers: will be responsible for maintenance of local scanning procedures including assessments of compliance, and will ensure that scanned records, born-digital records and paper records are accorded equal value and are adequately captured within recordkeeping systems.
Scanning Operators will be responsible for the actual scanning of files. These staff will also be involved in the preparations of files for scanning, quality assurance checking, and destruction in accordance with the Council's Confidential Waste procedures. Where possible roles will be segregated to ensure that one individual is not responsible for all aspects of the scanning process. Scanning operators will be trained to ensure they attain the appropriate competency level.

9 Storage technology and file formats

Whether or not the scans have been created in accordance with BS 10008, the resultant data should be managed in accordance with the Corporate Digital Preservation Policy to ensure its continued availability, and stored in a system which is capable of maintaining the characteristics of authentic records including a sustained audit trail. Unless departmental scanning procedures recommend otherwise, the Council's EDRM system should be used for storage, as it has a robust framework of access permissions, retention rules, and auditing to ensure it serves as a system capable of capturing and maintaining authentic records.

10 Monitoring, Auditing and Review

Monitoring of compliance with BS 10008 will be based around the requirements of the BIP0009 Compliance Workbook.
Audit services will assess scanning processes during visits.

A formal annual review of the scanning environment at the Derbyshire Business Centre will be undertaken and a report produced. This will help to identify non conformities. These will be reported to the Information Governance Group.

A management review of compliance with the Corporate Scanning Policy will be undertaken at regular intervals and reported to the Information Governance Group.
Any risk assessments undertaken in accordance with this policy shall be recorded and regularly reviewed.

Known conformity issues will be assessed to establish the impact of the issue and appropriate safeguards will be put in place.
This policy will be reviewed annually.

This document is owned by the Information Governance Group and forms part of the Council's ISMS Policy and as such, must be fully complied with.