Scanning Guidelines

Records Management
April 2017

for compliance with Code of practice for legal admissibility and evidential weight of information stored electronically (Reference document BSI document: BS10008)

Document Control Sheet

Name of Document:	Scanning Guidance, Records Management
Author	Alison Morris, Records and Heritage Manager (previously Eleanor Rowe, Records Manager)
Consultees	Mhairi Reilly, SharePoint Project Manager Sheila Strong, Mailroom Supervisor
Description of Content	To ensure compliance with legal admissibility guidelines and standards
Distribution:	Council wide – on intranet under Reference/Records Management Intranet – RMP Element 5 Appendix 11
Status	v 2.0
Date	April 2017

Contents

1.0 Introduction and Principles 3

1.1 Exceptions 3

1.2 Storage Media and file formats 3

2.0 Scanning Process 3

2.1 Scanning Quality Control Checks 3

2.2 Job Preparation 4

2.3 Scanning 4

2.4 Indexing – creating index entries/metadata for captured information 5

2.5 Original Document Storage after Scanning 5

3.0 Retention & Disposal 5

4.0 Authenticated copies 6

5.0 Physical equipment maintenance 6

6.0 Date and time accuracy 6

7.0 Information Security compliance 7

References 7

1.0 Introduction and Principles

The principles agreed for the handling of paper mail, as part of the implementation of a corporate document and records management system, are as follows:

- The address on return envelopes or quoted as the contact address on any documentation or website would be the central mail room address
- On receipt these items would be scanned and electronically transferred to either the appropriate work queue or individual as agreed with the relevant service.
- Any task thereafter would be instigated from the electronic image, the corporate mail room would deal with the paper in accordance with agreed rules in relation to retention – i.e. how long to keep, when to destroy etc

1.1 Exceptions

The following provides a flavour of the scenarios arising that resulted in exceptions being implemented:

- Process when paper and wet signatures are required, for example for a lease. The lease is issued for the client signature, which once signed is duly returned to the corporate mail room, but then requires the Council's signature to formalise the agreement. In these types of scenario the paper is passed to the service as there is no benefit in scanning a half complete lease.
- Plans – initial and final plans are scanned but amendments/variations in-between are not. This is to avoid unnecessary data on the system and because planners currently use the paper copy on site visits, so if plans were scanned they would only be printed off before a site visit anyway.
- Mail marked for the personal attention of an individual is initially passed, unopened, to relevant service.
- Back office process not developed to receive tasks electronically. An example is invoices, which are scanned after the processing work has been completed, it is worth noting that in this example e-invoicing is an initiative that will reduce paper in the future

1.2 Storage Media and file formats

All electronically stored information is held in PDF, Word, Excel, photographic type (TIFF, JPEG) format according to how the document originally created or scanned and imported e.g. Scanned correspondence will be in PDF format, but newly created and stored documents in the system may be in Word or Excel depending on their use.

2.0 Scanning Process

2.1 Scanning Quality Control Checks

Prior to scanning undertake quality control checks:

- scan a sample document and either compare it with a test target sheet or with the original for legibility, accuracy and alignment. It is recommended that all test scans are compared with original document.
- Keep a record of the result in the scanner check log.

2.2 Job Preparation

Prepare hard copy material ready for scanning:

Complete index/metadata that records batch number and details of the documents scanned, any special notes, etc

Check physical state of originals
Remove paperclips, elastic bands, staples, treasury tags, etc, ready for batch preparation and batch scanning. All folded, booklet-type, documents should be split into individual pages – a guillotine is the quickest and neatest way of doing this.

Record any material that is unsuitable for scanning either due to physical features (damage, size) or to copyright restrictions.

Record the numbers of pages in each document, remembering that a double-sided sheet counts as 2 pages.

Procedures should be in place to ensure that all pages of a multi-page document are kept together and in appropriate order before, during and after scanning

Check for post-it notes, tippex/correction fluid, fax, photocopies, amendments, alterations, coloured pages, alterations to signatures and record these in the notes associated with the scanned image. Check for any writing in other than black ink – this may not show up on a scan.

Assign a retention period and fate to the documents to be scanned. This will be recorded in the metadata to ensure the documents are not held permanently on the system.

2.3 Scanning

Fan and straighten batch to prevent jamming and multiple copies being fed through.
Double sided or single sided
Colour, greyscale or black & white
Ensure documents feed in straight
Check scanned images for obvious errors
Mark and identify those documents chosen as Quality Control tests
Complete Profile (metadata) for the documents created
Save documents and name according to file plan and naming conventions
Re-scanning – procedures in place for replacement of original if re-scanning necessary
Assign a retention period to the scanned images using appropriate metadata
Name of operator (if not retrievable from system login).
Quality checking undertaken

End Scan Procedures
Make a note of total pages scanned
Name of operator if appropriate
Quality checking undertaken

2.4 Indexing – creating index entries/metadata for captured information

Accurate indexing is crucial to allow electronic records to be retrieved. Complete the record profile (metadata) consistently and according to relevant file plan(s) and naming convention(s).

Manual indexing should be carried out by trained staff accurately and consistently. It should be checked for accuracy – spell checked, spot checks by senior admin staff, self-checks by data inputter. Where the copy could be required in any legal process then more experienced staff should be used to carry out the scanning process.

2.5 Original Document Storage after Scanning

Keep original documents that have been scanned batched together.
Identify box files/boxes with details of the original documents – record the following information on the box label:

- Date of scanning
- Batch numbers
- Type of document, e.g. Timesheets, correspondence with dates
- Date documents are due for destruction/disposal
- Quality control checks done

3.0 Retention & Disposal

Original documents that are destroyed after scanning should be kept for at least as long as is necessary to quality check the scanned image against the original and to ensure that the electronic copy has been successfully written to electronic storage and appropriate back-up procedures and quality control have been completed.

The Retention and Disposal Schedule will specify when an original document may be destroyed after it has been scanned, this is usually between 4-6 months. The Schedule is available on the intranet:
http://intranet.moray.gov.uk/Information_management/records_management.htm

There are exceptions and in these cases the original document should be retained for the full length of time indicated on the Schedule. These exceptions apply to:

- ○ Poor quality original paper documents for which a satisfactory image has not been obtained
- ○ Original paper documents that would require considerable enhancement for a good image to be achieved
- ○ Original document containing physical amendments or annotations that cannot be identified as such on the scanned image
- ○ Documents with physical amendments that have not been captured
- ○ Original records are retained for legal reasons e.g. signed contracts
- ○ Original documents not owned by The Moray Council and are returned to originator
- ○ Original documents where fraud is suspected or litigation is envisaged or pending

Once the date for destruction/disposal has been reached the original documents must be destroyed according to Record Management policy, and, a Destruction of Records

Authorisation Form should be completed and signed by the Senior Administrator. All available on the intranet via the above link.

Check with the Records and Heritage Manager before destruction if record(s) may have historical value.

4.0 Authenticated copies

If a copy of a scanned record is required it must be as accurate, and, be a good and faithful representation of the original.

For example if a copy is required for legal reasons it should be reproduced at the same resolution as the original scan. The stored image may be displayed in a different format for display that may lead to loss of information or differences in layout e.g. differing pagination or font size.

The authenticated copy produced from the scan should be authorised by senior staff.

5.0 Physical equipment maintenance

It is essential to ensure that the scanner is tested to ensure that it is working accurately to capture the best quality image of the original paper record and to ensure compliance with BS10008.

Remember to check the scanner at each operation for any debris, scratches etc and to clean it as necessary in accordance with the manufacturer's instructions.

6.0 Date and time accuracy

Accurate dating and timing of documents is crucial to their value as a record with integrity. Mark all appropriate records with date and/or time, e.g. all correspondence should contain the date – day, month and year.

Some data files may have embedded macros, which means that they will be modified each time they are opened e.g. the date may change to 'today’s date' if the current date field is self modifying. Evidence of the original date may therefore be lost, unless it can be retrieved from existing document metadata. This may cause problems if the document is required for legal or audit purposes as the original date may be overwritten. Do not use self modifying codes in documents unless these can be set so they do not automatically update a document when it is opened.

7.0 Information Security compliance

Please see the Corporate ICT Security Policy for further details.

Procedures should be in place to ensure that the integrity of any data files transmitted between systems cannot be compromised or altered and include an audit trail of the time and date of transmission. This should be controlled by the application software and include a checking mechanism e.g. a receipt or digital signature that all files transmitted have been received without alteration. Where confidentiality is important files could be encrypted during transmission.

References

Code of Practice for Legal Admissibility and evidential weight of information stored electronically BS10008

Moray Council Corporate ICT Security Policy

Records Management Policy and Strategy