Guide on the Identification and Disposal of Confidential Waste

Information Assurance Group

May 2019

Version 2.1

Document Control Sheet

Name of Document:	Guide on the Identification and Disposal of Confidential Waste
Author	Alison Morris, Records and Heritage Manager
Consultees	Information Assurance Group: including; Kathryn MacPherson, Senior Solicitor; Mike Alexander, ICT Security Officer; Atholl Scott, Internal Audit Manager; Sheila Campbell, Principal Librarian
Description of Content	Guidance for staff on the Council's responsibilities for the Secure and appropriate destruction of confidential waste, with mind to the Freedom of Information (Scotland) Act 2002, Environmental Information (Scotland) Regulations 2004 and the Data Protection Act 2018
Distribution:	Council wide upon approval
Status	Version 2.1
Date	~~Aug 2008 July 2014~~ May 2019

Contents

1.0 Introduction

The word ‘confidential’ will be used in this document to mean Confidential, Personal, Sensitive or Commercially Sensitive Records.

This guidance applies to all council staff. It is the responsibility of all staff to ensure that information is identified as confidential and destroyed effectively, securely and according to these guidelines.

This guidance applies to all records regardless of their format; including emails, databases, paper files, electronic files, CCTV, video and all other formats. Remember that if a paper copy is destroyed that a backup or corresponding electronic version must also be destroyed.

This guidance relates to confidential records:

- which need to be disposed of securely but which have not been filed
- documents that are records and have been filed in a recognised filing system (paper or electronic) and which must be disposed of according to the Council Record Retention Schedule: Element 5, Moray Council's Records Management Plan

Note: all records held by the Council can be requested under Access to Information legislation, including the Freedom of Information (Scotland) Act 2002 (FOISA), Environmental Information (Scotland) Regulations 2004 (EISR), and, Data Protection Act 2018 (DPA).

The unnecessary retention of documents and records takes up space, time and equipment and also makes dealing with Access to Information requests harder as more information has to be searched, and, potentially produced and redacted.

When disposing of records ask yourself – how serious would the consequences be to the person named in the document, the council, its staff, and service users if the record became freely available?

Remember identity theft is also a concern and we should not make it easy to obtain any personal details, such as names, addresses, telephone or signatures.

Be Waste Aware – this policy aims to maximise the amount of paper waste that can be recycled safely.

The person to contact in the Council regarding the destruction of confidential waste is: Records & Heritage Manager, records@moray.gov.uk Ext 2633

The company who has been awarded the contract to dispose of confidential waste for the council is: Shred-it.

2.0 Legislation

Records (paper or electronic) must not be destroyed if they are subject to litigation or an access request under the FOISA, EISR or DPA.

2.1 Data Protection Act 2018

Under Data Protection Legislation (including DPA and the General Data Protection Regulation (GDPR)) personal information must be:

- **Processed lawfully, fairly and in a transparent manner.**
- **Collected for specified, explicit and legitimate purposes.** (Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is ok.)
- **Adequate, relevant and limited**.
- **Accurate** and, where necessary, **kept up to date**; errors are **erased or rectified** without delay.
- **Kept no longer than is necessary** (stats, historical archiving exempt).
- **Held with appropriate security;** including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

2.2 Disclosure Scotland

The Code of Practice issued by Scottish Ministers concerning Disclosure has certain standards which must be met in the handling, processing and destruction of records.

Under the Code of Practice, Disclosure information:-

- Must be kept securely
- Where a disclosure is required in order to make a recruitment decision, must not be retained for any longer than is required after recruitment decision has been made
- Must be kept in a secure location until destroyed
- Must be destroyed securely and completely

Disclosure Scotland have the right to audit the council's handling, holding and destruction of Disclosure information; the Council must also have a written policy on handling, holding and destroying such information.

3.0 Record Retention & Bulk Disposal of Confidential Material

The Records Retention Schedule gives guidance on how long to keep records prior to disposal either by secure destruction or by transfer to the Archives.

The record retention schedules also make the council compliant with DPA as records will not be kept for longer than necessary prior to disposal. They are also

a requirement under Element 5 of the Council's Records Management Plan, required for compliance with the Public Records Scotland Act (2011). The schedules are available online under Element 5.

Bulk disposal of records by departments should be avoided as records should be reviewed regularly, nonetheless there can be requirements for bulk disposals and this is handled as an ad hoc collection of extra bags for secure destruction. Details on how to organise this are on the intranet under 'Records Management' or alternatively please contact Carol Grant or the Records and Heritage Manager for more information.

The Closed Records Store (CRS) will handle the majority of bulk destructions as the CRS manages semi-current records that are already identified as serving their retention periods. The review and destruction of these records is managed by Records and Heritage Manager, although departments will be consulted before their records are securely disposed of.

4.0 Recording Documents to be Destroyed

The Code of Practice on Records Management issued under FOISA states that a record of documents destroyed must also be kept. The Code states that the record of destruction should include – the reference, description, reason for destruction, date of destruction and authorisation for destruction.

You do not have to keep a record of each sheet of paper placed into the confidential waste consoles supplied by Shred-it.

The retention schedules will make the task easier as destruction is part of an agreed procedure in your department. This process is handled by the Records and Heritage Manager for the disposal of records that have reached the end of their retention dates in the Closed Records Centre.

However, if you do place a series of official or filed records either in the console or you ask for a bulk destruction - you should use the Destruction of Records Authorisation Form on the intranet. A designated officer should sign that the records are authorised for destruction.

Shred-it will provide Certificates of Destruction once the material has been destroyed; these should be retained.

If you are unsure please contact the Records and Heritage Manager.

5.0 Identification of Confidential, Personal, Sensitive or Commercially Sensitive Records

5.1 Confidential Records

Confidential records will include but are not limited to; personnel records, payroll records, bank account and salary details, drafts of policy documents which have not been agreed, documents with security implications, business records, legal records, medical, social work, education and pupil records, employee records and also CCTV and video etc.

Some records will also have Government security ratings and these should be observed.

5.2 Personal Data, including Special Category (sensitive personal) data

Personal data: Any information relating to an individual, particularly information that can be used to identify them such as: a name, an identification number, location data, an online identifier; or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. It also includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual – e.g., a manager's assessment of an employee's performance during their probation period.

Special Category Data (also referred to as **Sensitive Personal Data**): This is personal data consisting of information as to any of the following:

- Racial or ethnic origin.
- Political opinions.
- Religious or philosophical beliefs.
- Trade union membership.
- Genetics.
- Biometrics (where used for ID purposes – e.g. fingerprints).
- Health.
- Sex life.
- Sexual orientation.

Special category personal data is subject to much stricter conditions of processing under DPA. Personal data relating to criminal convictions and offences are not included but similar extra safeguards apply to its processing.

5.3 Commercially Sensitive Records

This may include reports, consultation documents, legal agreements, documents involving third parties, business records and drafts of documents which have not been published.

6.0 Recognising and managing the risks

6.1 Sort your records appropriately

Different methods of destruction will apply so take the time to sort out your records for destruction appropriately – don't be tempted to put everything for confidential disposal as this will have cost and time implications for your department.

Consider the level of risk if personal, confidential or commercially sensitive information became easily and widely available:-

- **low risk** – e.g. information already available or has been published.
- **medium risk** – e.g. draft policy documents or draft minutes which have not yet been approved, research not yet published.
- **high risk** – all confidential, personal, sensitive and commercially sensitive records. This could include documents such as printed out emails, letters, bank statements, personnel records, payroll records, education and pupil records, social work records, housing records, certain planning documents, regeneration records, membership details, commercial and business records, consultations, legal documents, agreements, policies, negotiations etc.

6.2 Dispose of your records appropriately

- **low risk** material does not need to be shredded prior to being recycled; it can be recycled according to the council's recycling procedures.
- **medium risk** material common sense will dictate whether material in this category may be recycled or should be stored and destroyed via the confidential waste consoles.
- **high risk** material that does not need to be retained for any retention period should be placed in the confidential waste consoles, as soon as they are no longer required.

Please note that for normal paperwork **no sorting is required** for paper placed into confidential waste consoles; paper clips, all coloured paper, staples, file folders, brochures, catalogues and even phone books can all be placed into the consoles.

Magnetic media, such as CDs, floppy disks, hard drives are handled separately, please contact the Records and Heritage Manager for advice on the disposal of these.

7.0 Destruction of Electronic Records

When deleting information from your computer hard drive it will probably go into the recycle bin – remember to regularly empty the recycle bin on your computer.

It will be the responsibility of departments to delete and destroy information held electronically, such as on shared drives and databases. It is also a department's

responsibility to ensure that permissions to such shared drives and databases are correct.

Remember that the retention schedules also apply to electronic records and that electronic files will need to be disposed of too.

7.1 Recording the Destruction of Electronic Records

The same principles should be applied to recording the destruction of electronic records as are applied to the destruction of paper records (see Section 4.0 for further information).

In the case of records stored on SharePoint this is achieved by keeping a document's metadata intact as a marker of its existence while deleting the document itself. However, no two electronic record systems are identical and this exact outcome may not be possible to achieve or necessarily be the best approach to take. A common sense approach should be taken when deciding how best to record the destruction of electronic records. If you are unsure please contact the Records and Heritage Manager.

8.0 Reminders

- Duplicate and/or backup copies stored on alternative media must be destroyed at the same time, in order to ensure compliance with DPA, Disclosure Scotland and FOISA legislation.
- Departments will be charged for the commercial service disposal of confidential material, so it is important to identify and dispose of only confidential waste in this manner.
- All confidential waste should be destroyed using the confidential waste consoles or extra bags supplied. Note that this should not include material classed as 'Low Risk' under Section 6 of this guide, which should instead be recycled according to the Council's recycling procedures.
- Confidential waste must be stored securely until destruction. Confidential waste placed in the Shred-it cabinets will be secure until collection.
- Keeping records according to the retention schedules will cut down on the amount of waste to be destroyed and ensure that a planned programme of destruction is implemented and kept to.
- Remember some records must be permanently preserved as archives. Refer to the retention schedules or the Records and Heritage Manager for advice.

9.0 Contacts

Records and Heritage Manager
Elgin Library
records@moray.gov.uk
01343 562633

Carol Grant
HQ
Carol.grant@Moray.gov.uk
01343 563391

10.0 References and Links

Moray Council's Website pages:

Information Management
http://www.moray.gov.uk/moray_standard/page_41220.html

Moray Council's Intranet Pages:

Information Security (inc. FOI, DPA)
http://intranet.moray.gov.uk/Information_management/information_security.htm

Records Management (inc. Retention Schedules, Confidential waste etc.)
http://intranet.moray.gov.uk/Information_management/records_management.htm

BS ISO 15489:2016 – Records Management

BS EN 15713:20098470:2006 Secure Destruction of confidential material

ISO EN 9001:2015 Quality Management Systems

11.0 Flow chart

Flow chart illustrating the destruction of Confidential, Personal, Sensitive and Commercially Sensitive Records. (**Note**: flow chart specifies procedure for paper records. Please consult Section 7 for further information on electronic records. Guidance given throughout generally applies to both paper and electronic records.)