

Confidential Waste Policy

Document control		
Document title	Confidential Waste Policy	
Purpose	Information Security	
Author		
Date of publication		
Valid until	04/06/2018	
Owner/responsibility	Nicola Welch/Peter Hogg	
Distribution	LanConsent/Other	
Version	Date	Comments
Version 1.0	May 2011	
Version 2.0	June 2018	New working practices and policy references GDPR requirements



Disposal of Confidential Waste Policy

1. Introduction – Why do we need this policy?

The Council has a statutory duty to protect personal and sensitive information it holds and manages and this policy sets out Wigan Council's approach by which personally identifiable or organisationally sensitive information (either paper based or electronic) is disposed of in a controlled and secure manner.

This policy provides a consistent approach to the way in which we handle and dispose of confidential waste.

The sixth principal of the General Data Protection Regulation concerns the destruction of confidential waste, which states:

Data should be processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

2. Associated Policies and Procedures – What other guidance is there?

This policy supports existing Council information governance procedures that relate to the protection and security of data. A range of policies already provide advice and guidance concerning the Council's minimum standards for the protection of data, i.e.

Data Handling Framework
Information Risk Policy
Wigan Council's Data Protection Policy
IT Security Policy
ICT Services Acceptable Use Policy
Use of Mobile Data Devices & Equipment Policy

3. Aims and Objectives – What is this purpose of this policy?

The careless storage and disposal of personal and sensitive information could result in breaches of confidentiality, therefore the purpose of this policy is to ensure that confidential records are disposed of in an appropriate and secure manner and that no information is inadvertently disclosed.

4. Scope of the Policy – Who and what does this policy apply to?

Who

All Council staff, members, external contractors, partners and volunteers working on behalf of the Council who have access to personal or sensitive data must observe the requirements of this policy.

What

These procedures apply to the disposal of information stored on all types of media, whether this be in paper or electronic form.

5. Definitions – What is personal, sensitive and confidential data?

Personal data:	means data which relates to a living individual who can be identified, e.g. name, address, dob, identification number, location data or online identifier. It will also apply to personal data generated automatically.
Personal sensitive data:	contains personally identifiable data and other more personal data such as a persons ethnic origin, health, political opinions, religious or philosophical beliefs, trade union membership, details of a person's sex life or sexual orientation.
Business sensitive data:	may include information that should not be disclosed due to political or financial reasons, e.g. contract tender.
Confidential data:	is any data that falls into the above categories. However, whilst not officially classed as confidential, other information has the potential for misuse, e.g. official blank forms or headed paper that could be misused, so you should be thoughtful of this when assessing their classification.

6. Who can I contact for advice?

If you have any doubt about the how best to classify or dispose of information contact your line manager, IT Service Desk, the Council's Data Protection Officer or Internal Audit.

7. How do I dispose of electronic IT waste?

In accordance with Section 7.8 of the IT Security Policy all obsolete or redundant Council IT equipment and devices used to store Council information must be returned to the IT Service for disposal.

This requirement extends to, but is not limited to, equipment such as:

- PC's
- Tablets
- CD / DVD's
- Mobile phones
- Laptops
- Pen drives
- Faxes
- External portable hard drives
- Media tapes
- Printers

Where possible the stored information should be erased prior to delivery to the IT Service for secure disposal. Please refer to the ICT helpdesk details below:

Contact Details for the ICT Helpdesk.

Telephone Number: 4142 (01942 404142).

ICT Self Service Log in: <https://itportal.agisw.co.uk>

8. How do I dispose of confidential paper waste?

8.1 Shredding

The use of shredders is permitted as long as a '**Cross Cut Shredder**' is used. This type of shredder cuts the paper into small strips or fine particles to prevent information from being obtained from the document.

Once correctly shredded, the waste does not need to be disposed of through the confidential waste route and should be considered for recycling.

8.2 Contractor Disposal (From 29th May 2018)

- ***Introduction***

The following confidential waste disposal procedures should only be used for confidential paper waste and any other sensitive paper material. They should not be used for the disposal of general paper or domestic waste.

Rapide Reprographics Ltd are the Council's official contractor for dealing with confidential waste paper disposal

Rapide Contact details

E-mail: sales@rapide-repro.co.uk

Tel: 0845 257 00 22

Fax: 0845 257 00 33

- ***Sacks***



The official Rapide sacks must be used for the disposal of bagged confidential waste. The print on these sacks is in **bold red letters** to indicate that they are for confidential waste.

Take care not to make the sack too heavy – as a guide, it should not be too difficult to pick up and transfer the sack with one hand.

Sealing of Sacks

Each sack must be tied with cable ties which can be obtained from any store

Unsecure sacks will not be collected and replacement ties are supplied by Rapide after each collection.

Containers

Lockable containers can also be provided by Rapide. The containers have a slot in the top for the paper.

The keys for these lockable containers must be kept secure at all times.

Each container will have a plastic disposal bag inside which will be securely tied by Rapide before it is taken from the building.

Storage

All confidential waste awaiting collection must be held securely within the premises to prevent unauthorised access or disclosure.

If a secure storage and collection point within the building can be determined then this area should be used.

The confidential waste must not be left outside awaiting collection.

Note: On no account should any confidential waste be placed with other general waste, even if secured.

Arranging Collection

Staff should contact Facilities Management email address (FManagement@wigan.gov.uk) if they require a collection or more containers/sacks. Rapide deliver and collect on Tuesdays and requests should be made to FM the Friday before the Tuesday.

All Town Halls have scheduled collections, but if staff require more containers/sacks, again they should email Facilities Management.

On Collection and Record Keeping

All collection and disposal details are stored Rapide's online service website and can be accessed via Facilities Management. These records are kept for 2 years.

9. Policy compliance

This policy should ensure that confidential waste is managed and disposed of in the most secure manner and it is everyone's responsibility to ensure that confidential and personal information is kept safe from disclosure.

If you become aware that an information security breach has taken place inform your Head of Service and Data Protection Officer immediately.

Non-compliance with this policy may be subject to formal action under the Council's disciplinary procedure and may constitute gross misconduct where appropriate. This could ultimately lead to dismissal from employment.