

Confidential Waste Policy

Responsibility for Policy:	Registrar and Chief Operating Officer
Relevant to:	All LJMU Staff
Approved by:	ELT
Responsibility for Document Review:	Director of Campus Services
Date introduced:	15 th June 2021
Date(s) modified:	June 2023
Next Review Date:	June 2024

RELEVANT DOCUMENTS

- Data Protection Act 2018
- UK GDPR 2021

RELATED POLICIES & DOCUMENTS

- Data Protection Policy
- Information Security Policy
- Staff Handbook
- Code of Conduct for Staff
- Disciplinary Procedure

Confidential Waste Policy

1 Purpose

This policy sets out the University's approach to disposing of confidential waste. It informs staff of their responsibilities and how LJMU will enable these to be met.

2 What is Confidential Waste?

The term confidential waste in this policy is used to cover all information that is private to LJMU and not public knowledge. Some things will be obvious as they contain personal data, sensitive personal data or information obtained under a duty of confidence.

Not all information contains personal data but may still require confidential disposal because it contains commercially sensitive or business information.

LJMU requires that all confidential waste is disposed of securely and appropriately.

Examples of information which require secure disposal

- Personal Data – names, addresses, date of birth, lifestyle, photographs
- Bank details and financial information
- Confidential Information
- Working Papers (containing confidential or personal information)
- Draft Documents (containing confidential or personal information)

3 Data Protection and GDPR

Organisations must have appropriate technical and security measures in place to protect the personal data that they process.

Disposing of waste containing personal data is processing under the Data Protection Act 2018 and the UK General Data Protection Regulation (GDPR) and therefore we must ensure that confidential waste is kept secure and protected against accidental loss, damage and under authorised access up until it is finally destroyed.

Confidential waste must be kept separate from other waste and handled in accordance with this policy.

4 Records Retention Schedule

The appropriate time for keeping information held at LJMU can be found in LJMU's [Records Retention Schedule](#) in the University Policy Centre. The retention period applies equally to all media, including electronic.

Secure destruction is an expensive process therefore non-confidential material should be disposed of in general paper recycling.

Examples of information which does not require secure disposal

- Newsletters
- Press Releases
- Information already in the Public Domain

5 Responsibilities

5.1 All staff

Everyone is responsible for the personal data and business information that they use on a daily basis and are under a duty of confidentiality under their contract of employment.

Staff must comply with the LJMU Data Protection Policy and their responsibilities under the GDPR at all times.

Staff must ensure that confidential waste is kept secure at all times and the correct process for disposal as set out in this policy is followed. Confidential waste consoles are provided throughout each Campus area for the secure disposal of general day to day waste. All staff should ensure these are used for confidential waste items. Confidential waste should not be put into the general waste bins. Where larger scale confidential waste removal is planned, the procedures outlined in section 6 must be followed.

Staff should raise any issues of concern regarding the management of confidential waste with managers and supervisors

Any breach of this policy should be classed as a security incident and should be reported to the Data Protection Officer at DPO@LJMU.ac.uk in line with the [Personal Data Breach Policy](#).

5.2 Executive Leadership Team

- To ensure compliance with the GDPR at all times.
- To ensure managers and supervisors within Faculty and Service Teams are responsible for the management of confidential waste and confidential waste collections.
- To ensure the promotion of data protection and compliance with policies through the University governance structure.

5.3 Managers and Supervisors

- To ensure that all staff are aware of their responsibilities under the GDPR regulation and are complying with those responsibilities.

- To raise any matters of concern regarding Data Protection with the Data Protection Officer.
- To ensure that certificates of destruction are retained for all direct collections and uploaded to the Data Protection SharePoint site.
- To ensure the successful operation of this policy.

5.4 Data Protection Advisors Group

- As members of the Data Protection Advisors Group, they disseminate data protection policies and updates from the Data Protection Officer within their Faculty and Service Teams and advise on Data Protection matters at a local level.

5.5 Estate and Facilities Management

- To manage the confidential waste collection contract, ensuring certificates of destruction have been provided for all collections.
- To develop procedures for confidential waste collection within Faculty and Services Team in accordance with this policy
- To raise any matters of concern regarding Data Protection with the Data Protection Officer.

5.6 Data Protection Officer

- To inform and advise the University of its obligations under the GDPR.
- To monitor compliance with the obligations under GDPR and with the University's policies and procedures in relation to the protection of personal data. This may include carrying out audit checks to ensure that policies are being adhered to.

6 How to dispose of Confidential Waste

6.1 Use of Confidential Waste Boxes

- There are dedicated confidential waste boxes across the University. You must dispose of day to day confidential waste through these secure confidential waste boxes. These are positioned across University buildings. Managers and Supervisors will advise of locations.
- Confidential waste is collected from the designated locations on a monthly schedule by the appointed confidential waste supplier.
- The confidential waste supplier will securely remove the waste, in line with secure chain of custody arrangements and provide a certificate of destruction for each collection once offsite destruction has been completed
- CDs, floppy disks, audio and video tapes that need to be disposed of as confidential should not be placed into confidential waste consoles but be bagged up separately and securely from paper waste. Please log a

helpdesk request via the Estates & Facilities Management helpdesk for uplift of these types of waste.

- Please remove documents from folders, plastic/ paper wallets, box files, poly pockets, paper clips, treasury tags before being sent for destruction.
- Small amounts of very sensitive information may be shredded at department level.

6.2 Use of Confidential Waste Bags

- Confidential waste bags are to be used in exceptional circumstances when there is a large amount of confidential waste to be disposed of. This could be part of a refurbishment and/or an internal move.
- Confidential waste bags should be requested via the Estate and Facilities Management Helpdesk.
- Bags are not to be overfilled, and should be half full. They will be removed in accordance with manual handling risk assessments and processes
- The confidential waste bags must be sealed and secured at all times.
- Confidential waste bags can be directly collected by our confidential waste supplier if there are 10 or more bags ready for collection. Where there are fewer than 10 bags ready for collection, these will need to be stored in a local secure holding area assigned by Campus Services
- Your confidential waste bags must be kept secured and a job raised on the Estates & Facilities Management Helpdesk for collection. They must remain secured whilst collection by the confidential waste supplier or Campus Services is arranged
- Where Campus Services are required to move bags to the temporary secure holding area, the person responsible for the confidential waste (waste producer) or the person who has raised the requests via the helpdesk must be in attendance to escort the waste to the temporary holding area to ensure a secure chain of custody.
- The confidential waste supplier will attend and securely remove the waste either directly from the Faculty or Service Team or from the Campus Services temporary secure holding area and provide a certificate of destruction for each collection.
- CDs, floppy disks, audio and video tapes that need to be disposed of as confidential should be bagged up separately and securely from paper waste. Please log a helpdesk via the Estates & Facilities Management helpdesk request for uplift of these types of waste.
- Please remove documents from folders, plastic/ paper wallets, box files, poly pockets, paper clips, treasury tags before being sent for destruction.

- Small amounts of very sensitive information may be shredded at department level.

7 Certificates of Destruction

7.1 Retention Period

- Certificates of Destruction are required for confidential waste collections. They are to be retained in accordance with the Records Retention Schedule.

7.2 Location of Records

- Managers and Supervisors are responsible for ensuring that the certificates are received at each collection and uploaded to the Data Protection SharePoint site.

8 Review

This policy will be reviewed annually