



# Nottinghamshire County Council

## Policy Library Pro Forma

This information will be used to add a policy, procedure, guidance or strategy to the Policy Library.

**Title: Confidential Waste Procedure**

**Aim / Summary:** To ensure the Council has procedures in place to ensure the secure disposal of confidential waste generated or used by the Council.

**Document type** (please choose one)

Policy		Guidance	
Strategy		Procedure	X

**Approved by:** DPO

**Version number:** 1.1

**Date approved:** 30/7/19

**Proposed review date:** 15/02/2021

**Subject Areas** (choose all relevant)

About the Council	X	Older people	X
Births, Deaths, Marriages	X	Parking	X
Business	X	Recycling and Waste	X
Children and Families	X	Roads	X
Countryside & Environment	X	Schools	X
History and Heritage	X	Social Care	X
Jobs	X	Staff	X
Leisure	X	Travel and Transport	X
libraries	X		

**Author:** DPO

**Responsible team:** Information Governance

**Contact number:** 0115 804  
3800

**Contact email:**  
data.protection@nottsc.gov.uk

**Please include any supporting documents**

3. [The Data Destruction Standard](#)

4. [Information Compliance Policy](#)

**Review date**

**Amendments**

12 October 2016

Original approved by IGG

30 July 2019

Various to take account of new legislation and NCC policies and standards



# Confidential Waste Procedure

## At a glance ...

- All confidential waste should be disposed of securely and in line with this procedure.
- The Independent Inquiry into Child Sexual Abuse (IICSA) requires that the Council retains all records of potential relevance to the Inquiry, for the duration of the Inquiry. There is a [process for the retention and disposal of information during the IICSA inquiry period](#).
- The Council (through Catering & Facilities Management) employs a contractor ([Shredall \(East Midlands\) limited](#)) to securely destroy all paper-based confidential waste.
- Confidential waste must not be transported other than by a courier service arranged by Catering & Facilities Management.
- All confidential waste must be held securely pending destruction.
- Small volumes of paper confidential waste can be shredded using a shredder which conforms to DIN P-4
- Confidential waste stored electronically (e.g. on a hard drive) must be disposed of by ICT Services in line with the [Data Destruction Standard](#).

## Context

1. Nottinghamshire County Council (NCC) creates a significant amount of confidential waste. The [Data Protection Act 2018](#) requires the Council to ensure confidential waste with personal or sensitive personal information is disposed of securely.
2. The [Information Compliance Policy](#) requires the Council to appropriately dispose of paper and electronic information classified as personal or confidential using the appropriate standards and procedures.
3. It is important to note that the Independent Inquiry into Child Sexual Abuse (IICSA) requires that the Council retains all records of potential relevance to the Inquiry, for the duration of the Inquiry. There is a [process for the retention and disposal of information during the IICSA inquiry period](#).
4. Confidential waste may include information that is commercially or organisationally sensitive.
5. The Council (through Catering & Facilities Management) employs a contractor ([Shredall \(East Midlands\) limited](#)) to securely destroy all paper-based confidential waste.

6. There is currently no requirement for all Council sites to use the collection service arranged by Catering & Facilities Management, however all confidential waste should be disposed of securely and in line with this procedure.

## Definitions

7. **Confidential waste** is defined as waste that contains personal data or data that is considered sensitive to the Council's business. For example:
  - a. Personal data, as defined by the Data Protection Act 2018.
  - b. Finance information e.g. payroll, pensions or benefits.
  - c. Staffing information e.g. personnel files, occupational health records.
  - d. Commercially sensitive e.g. contracts, maintenance records.
  - e. Service user information e.g. care records.
  - f. Any information classified as Official or Official-Sensitive
8. It can be produced in a number of formats manual and electronic; paper, audio and video recordings, microfiche, photographs, image files, databases, CDs, DVDs, computer hard drives, removable data storage.
9. **Confidential waste bins** are bins provided by the Council for the sole purpose of storing paper-based confidential waste.
10. **Data** is reinterpretable representation of information in a formalised manner suitable for communication, interpretation or processing e.g. a number, word or symbol in a report, spread sheet or database.
11. **Destroy** is to eliminate or erase confidential waste beyond any possible reconstruction.
12. **Information** is knowledge concerning objects that within a certain context has a particular meaning.
13. **[The Data Destruction Standard](#)** is a Council procedure to ensure that the data stored on ICT equipment is securely deleted or destroyed, preventing the retrieval of that data under any circumstances.
14. **Portable storage devices** (for example USB sticks, iPods, PDAs, smartphones, digital cameras, and external hard drives) are devices that connect to the USB port of a computer and are used to store and retrieve data.
15. **A record** is information created, received, and maintained as evidence or information by the Council, in pursuance of legal obligations or in the transaction of business.
16. **Removable media** is any type of storage device that can be removed from a computer while the system is running. Examples of removable media include CDs, DVDs and Blu-Ray disks, as well as diskettes and USB drives.

## Scope of this procedure

17. This procedure applies to all Council buildings and locations.
18. This procedure applies to all confidential waste held by the Council, regardless of format. This includes documents and records in electronic or digital form as well as physical form (hardcopy).
19. This procedure applies to all elected members, officers and through commissioning and agreements, partners, volunteers, contractors and consultants.

### **Principles and Commitments**

20. The Council will ensure that:

- a. Confidential waste is disposed of in accordance with relevant legislation and statutory requirements.
- b. Information, data and records that are no longer required will be appropriately disposed of.
- c. All those working for or on behalf of the Council will be made aware of the need to dispose of confidential waste securely and in accordance with this Procedure.

21. It will do this by ensuring:

1. Paper confidential waste will be collected from Council buildings upon request to Catering & Facilities Management.
2. Where possible, small volumes of paper confidential waste can be shredded using a shredder which conforms to DIN P-4 as a minimum.
3. Prior to collection, paper confidential waste will be stored in bags in a secure location, with access restricted to only those with a business need to access it.
4. Paper confidential waste will be collected and transported only by a courier organised by Catering & Facilities Management.
5. Where paper confidential waste is not collected by courier, all confidential waste must be shredded before disposal.
6. Confidential waste stored electronically (e.g. on a hard drive) will be disposed of by ICT Services per the [Data Destruction Standard](#).

22. Employees and departments will do this by complying with the following:

1. Review any waste to assess if it should be considered confidential waste under Section 6 of this procedure.
2. Paper documents will be placed in confidential waste as soon as they are no longer serve a business purpose.
3. Confidential waste should not be left unattended when not in a secure location.
4. Where confidential waste has been disposed of incorrectly (e.g. put in standard recycling), C&FM should be contacted to retrieve this to be disposed of correctly.

5. If guidance is required on confidential waste, the Information Governance Team should be consulted via [data.protection@nottsc.gov.uk](mailto:data.protection@nottsc.gov.uk)
6. Staff wishing to dispose of ICT equipment should follow the ICT Disposal Procedure in Table 1 of the Data Destruction Standard, ensuring that where data destruction has been outsourced, a Certificate of Destruction is obtained.

### Responsibilities in relation to Principles and Commitments

23. The Council's [Information Governance Framework](#) sets out all of the key [information governance roles and responsibilities within the Council](#).
24. Additionally, the below have specific responsibilities relating to confidential waste:
  - a) **ICT Services**; are responsible for ensuring that ICT equipment is securely disposed of in accordance with the [Data Destruction Standard](#).
  - b) **Catering & Facilities Management**; The team will be responsible for ensuring all paper-based confidential waste is securely collected from all Council sites and destroyed.
  - c) **Solutions4Data, Mail & Despatch**; couriers working for this team will collect small amounts of paper-based confidential waste and return to County Hall for central collection and secure destruction.
25. All elected members, officers and through commissioning and agreements, partners, volunteers, contractors and consultants are responsible for complying with this procedure.

### Monitoring and Review

26. This procedure will be reviewed annually in line with legislation and codes of practice.

### Further Information

27. Specific requests for the collection / transportation / shredding of paper confidential waste can be made to:

Requests for the collection / transportation / shredding of paper confidential waste	Catering & Facilities Management Email: <a href="mailto:facilities.re@nottsc.gov.uk">facilities.re@nottsc.gov.uk</a> Tel: 0115 9773316
Queries on the destruction of electronic confidential waste	IT Service Desk Email: <a href="mailto:itservicedesk@nottsc.gov.uk">itservicedesk@nottsc.gov.uk</a> Tel: 0115 9772010
General advice on confidential waste and other information governance matters	Information Governance Team Email: <a href="mailto:data.protection@nottsc.gov.uk">data.protection@nottsc.gov.uk</a> Tel: 0115 8043800

### Document Control

<b>Owner</b>	Caroline Agnew, Data Protection Officer
<b>Author</b>	William Smith Information Manager
<b>Last Reviewer</b>	Brendan Jennings, Information Governance Advisor
<b>Approver</b>	Data Protection Officer
<b>Date of Approval</b>	30/07/2019
<b>Date of next review</b>	15/02/2021 [to tie in with provider contract duration]
<b>Version</b>	1.1
<b>Classification</b>	Public

<b>Version</b>	<b>Date</b>	<b>Changes</b>
1.0	12/10/2016	Original document approved by Information Governance Group
1.1	30/07/2019	Changes to incorporate greater detail on compliance standards required, new legislation and good practice