Confidential Waste Procedures

1 Version History details and author

1.0		Completed for Distribution	David Jenkins
2.0	14/09/2015	Approved by Information Governance Group	David Jenkins
3.0	10/10/2016	Approved by Information Governance Group. Addition of destruction of portable media.	David Jenkins.
4.0	06/11/2017	Reviewed by Information Governance group. Roles and responsibilities amended.	Mark Smith
5.0	03/12/2018	Reviewed by Information Governance Group. Links to Safe Haven Guidance updated.	Mark Smith
6.0	14/01/2020	Reviewed by Information Governance Group. Advice added re microform information. Unshredded waste not to be added to domestic bins.	Mark Smith
7.0	09/03/2021	Reviewed by Information Governance Group. Links amended.	Mark Smith
8.0	08/02/2022	Reviewed by Information Governance Group. No changes.	Mark Smith
9.0	07/03/2023	Reviewed by Information Governance Group. Scope changed to include special category data. Clarification given on what is confidential waste.	Mark Smith
10.0	09/01/2024	Reviewed by Information Governance Group. Onsite shredding removed.	Mark Smith
11.0	11/02/2025	Reviewed by Information Governance Group. Agency staff added.	Mark Smith

This document has been prepared using the following ISO27001:2022 standard controls as reference:

ISO Control A.5.10 – Handling of Assets
ISO Control A.5.12 - Classification of Information
ISO Control A.5.13 – Labelling of Information
ISO Control A.5.31 - Identification of applicable legislation
ISO Control A.5.36 - Compliance with security policies and standards
ISO Control A.6.3 - Information security awareness, education and training
ISO Control A.7.10 - Disposal of Media

2 Introduction

Derbyshire County Council creates and manages a great deal of personal and confidential information which will eventually require disposal. Poor management of the disposal of confidential waste exposes the Council to the possibility of a data breach which could incur financial penalties and reputational damage.

A variety of options exist for the disposal of confidential waste which will vary depending on where staff are based. Due to the number varying locations of DCC offices it is not possible to offer one single approach to confidential waste for the entire Council. These procedures outline the various options available to staff.

Confidential waste largely relates to paper documents however it can also include electronic information stored on external storage media (such as USB sticks, CDs, microform etc).

These procedures should be read in association with the Records Disposal Policy and Procedures and the Secure Destruction of Optical and Magnetic Media Procedures. These documents are available at: Record Disposal documents

3 Scope

These procedures apply to all Council staff, agency staff, volunteers and elected members who are disposing of confidential waste.

Confidential waste includes anything categorised under the Corporate Data Protection Policy as personal information, whether or not this includes Special Category data (medical information, sexual orientation, religion etc). Commercially or organisationally sensitive information should also be treated as confidential.

4 Roles and Responsibilities

It is the responsibility of all managers to inform their staff of the appropriate confidential waste arrangements which apply to their working area. They are also responsible for ensuring that staff adhere to the agreed procedures.

It is the responsibility of all council staff, employees, elected members, agency staff, volunteers and third parties to use the appropriate confidential waste method depending on their location within the Council.

5 Minimum expectations regarding disposal of confidential waste

Confidential waste should be secured appropriately prior to disposal. Staff should continue to manage their information according to the Safe Haven Guidance. Security measures can include placing waste bags in a locked container, or in a locked room where only those staff who are responsible for the waste have access to the room. This is to avoid confidential waste in unmarked bags/containers being disposed of as general waste by staff unfamiliar with local processes. Confidential waste should not be left unattended in places like corridors or reception areas.

Where shredders are used by offices they must be cross shredders. Any new shredders which are purchased should conform to this requirement. Offices should phase out strip shredders.

Confidential waste should be disposed of in a timely manner and should be regularly disposed of and not allowed to accumulate indefinitely.

Containers holding confidential waste should be emptied at regular intervals.

Domestic waste bags **should never** be used for the disposal of un-shredded confidential waste as these may be disposed of insecurely in landfill sites.

If waste is being transferred to another site for shredding it should not be left unattended during transit. For example, if a bag of waste is being transported from a smaller office to a larger office with confidential waste provision it should not be left overnight in a member of staff's car. For further guidance, see: Information security away from work and Working on the move.

Before disposing of information as confidential waste staff should check the appropriate records retention schedule to establish whether the information can be disposed of. Retention Schedules can be found at the following link: retention schedules.

It is acceptable to place shredded confidential waste in paper recycling.

Microform materials containing confidential information can be disposed of by the council's confidential waste contractor. If an office requires this service they should contact Records Management to make the appropriate arrangements.

Optical and magnetic media containing confidential information, such as computer disks, compact discs, USB sticks, audio and videotapes, should be disposed of using the Council's Secure Destruction of Optical and Magnetic Media Procedures.

6 Available methods for disposing of confidential waste

Confidential waste contractor - used by staff in the Matlock complex and in larger satellite offices - Waste is placed in lockable containers and collected by contractor at pre-arranged intervals. Keys to containers should be given to a limited number of staff. Only the approved DCC contractor should be used.

On-site shredding - Typically used by staff in area offices/libraries - Use of on-site shredders. Waste should be shredded as soon as practical. Shredded waste can be recycled. Cross shredders should be used. Confidential waste should not be left insecure or unattended prior to shredding.

Transferring to area hub - typically used by staff in small offices/HOPs - Waste (un-shredded) is transferred from a smaller site to a large one either for on-site shredding or disposal by contractor. Waste should not be left insecure before and after transfer. Waste must not be left unattended in a member of staff's vehicle. Only confidential waste should be placed in containers (not all paper waste).

The method of disposing of confidential waste will be determined by business requirements and location. If an office requires the use of the confidential waste provider they should contact Records Management to make the appropriate arrangements.

If offices are planning on disposing of a significant quantity of confidential waste (i.e. before an office move) then they should contact Records Management to discuss

which approach would be appropriate. In these instances it might be appropriate to use the confidential waste contractor for ad-hoc collections.

Electronic external storage media (e.g. USB memory sticks and CDs) can also be disposed of as confidential waste. To arrange the disposal of electronic media staff should contact the IT Service Desk to make appropriate arrangements.

7 How to determine what information is confidential waste

The content of a document will determine whether it is classed as confidential waste. All information classed as 'Restricted' must be disposed of as confidential waste. Information classed as 'Controlled' may require disposal as confidential waste, depending on content. In any case of doubt and especially if disclosure would cause damage to the council or distress to an individual, the information should be disposed of as confidential waste. Special Category data should be disposed of as a high priority.

Any potential breach of security involving confidential information caused by the inappropriate disposal of waste, should be reported by using the Council's Security Incident Reporting process.

8 Review and Monitoring

This procedure will be reviewed annually.

This document is owned by the Information Governance Group and forms part of the Council's ISMS Policy and as such, must be fully complied with.