

Disposal of Paper Confidential Waste

Issue Date	Review Date	Version
July 2018	July 2023	1

Purpose

This document sets out the process for staff in the management of paper confidential waste.

Who should read this document?

All staff that handle paperwork which contains personal information.

Personal information is information that can identify an individual, whether a patient, visitor or a member of staff.

Key Messages

- All paper confidential and sensitive waste must be disposed of only in the lockable blue bins provided.
- When the bin is three quarters full, an email should be sent to the address on the bin (Derriford Waste Management Solutions), to request a collection.
- Confidential waste bin keys should not be routinely kept by Trust staff, and in an instance where a document or item has been placed in the bin in error, a request for the bin to be opened must be made via a senior member of staff: i.e.: Matron, Senior Nurse, ED/Director on call, 355 on call, Service Line Manager.
- Keys will be kept at the parking desk on Level 6, and must be signed for and returned by one of the above named staff.
- If a document is placed in the bin in error, it must be treated as an incident and subsequently put on Datix.
- In exceptional circumstances, a request may be made to Information Governance for a key to be held in a specific area by a senior team member. That team member will then be responsible for that key and for ensuring its use is monitored.

Core accountabilities	
Owner	Assistant Operations Manager/Local Security Management Specialist Information Governance Support Manager
Review	Caldicott and Information Governance Assurance Committee
Ratification	Caldicott and Information Governance Assurance Committee
Dissemination (Raising Awareness)	Information Governance Support Manager Assistant Operations Manager/Local Security Management Specialist
Compliance	Information Governance Support Manager Assistant Operations Manager/Local Security Management Specialist
Links to other policies and procedures	
Information Governance Policy Safe Handling Management and Disposal of Hospital Waste Policy	
Version History	
V1	Initial Document

The Trust is committed to creating a fully inclusive and accessible service. Making equality and diversity an integral part of the business will enable us to enhance the services we deliver and better meet the needs of patients and staff. We will treat people with dignity and respect, promote equality and diversity and eliminate all forms of discrimination, regardless of (but not limited to) age, disability, gender reassignment, race, religion or belief, sex, sexual orientation, marriage/civil partnership and pregnancy/maternity.

An electronic version of this document is available on Trust Documents on StaffNET. Larger text, Braille and Audio versions can be made available upon request.

Standard Operating Procedures are designed to promote consistency in delivery, to the required quality standards, across the Trust. They should be regarded as a key element of the training provision for staff to help them to deliver their roles and responsibilities.

Section	Description	Page
1	Introduction	4
2	Definitions	4
3	Regulatory Background	4
4	Key Duties	5
5	Procedure to Follow	5
6	Document Ratification Process	5
7	Dissemination and Implementation	6
8	Monitoring and Assurance	6

Standard Operating Procedure (SOP)

Disposal of Paper Confidential Waste

1 Introduction

All employees working in the NHS are bound by a legal duty of confidence to protect personal information they may come into contact with during the course of their work in line with their contractual responsibilities and Data Protection legislation.

Confidential information within the NHS is commonly thought of as health information; however, it can also include information that is private and not public knowledge or information that an individual would not expect to be shared. Information can relate to patients and staff (including temporary staff), external contractors and University Hospitals Plymouth NHS Trust business.

This SOP sets out the process to follow when disposing of paper confidential waste.

2 Definitions

Paper waste which needs to be disposed of as sensitive and confidential falls into the following categories:

Documents and records containing personal/patient identifiable information:

Anything which contains the means to identify a person: name, address, postcode, date of birth, NHS number, care plan, staff payroll number, questionnaires or other data collected under an understanding of confidentiality etc.

Documents and records containing commercially sensitive information:

Commercially sensitive information is anything that relates to contracts, tenders, purchasing records, maintenance records, insurance, unpublished meeting minutes, draft policies etc.

3 Regulatory Background

- Data Protection Act 2018
- General Data Protection Regulation (GDPR)
- Common Law Duty of Confidence

4 Key Duties

Managers within the Trust are responsible for ensuring that all staff are aware of the process for disposal of paper confidential waste.

All staff, whether permanent, temporary or contracted and contractors are responsible for ensuring that they are aware of the requirements incumbent upon them and for ensuring that they comply with these on a day to day basis.

5 Procedure to Follow

- All paper confidential and sensitive waste must be disposed of only in the lockable blue bins provided.
- When the bin is three quarters full, an email should be sent to the address on the bin (Derriford Waste Management Solutions), to request a collection.
- Confidential waste bin keys should not be routinely kept by Trust staff, and in an instance where a document or item has been placed in the bin in error, a request for the bin to be opened must be made via a senior member of staff: i.e.: Matron, Senior Nurse, ED/Director on call, 355 on call, Service Line Manager.
- Keys will be kept at the parking desk on Level 6, and must be signed for and returned by one of the above named staff.
- If a document is placed in the bin in error, it must be treated as an incident and subsequently put on Datix.
- In exceptional circumstances, a request may be made to Information Governance for a key to be held in a specific area by a senior team member. That team member will then be responsible for that key and for ensuring its use is monitored.

6 Document Ratification Process

The design and process of review and revision of this procedural document will comply with The Development and Management of Formal Documents.

The review period for this document is set as default of five years from the date it was last ratified, or earlier if developments within or external to the Trust indicate the need for a significant revision to the procedures described.

This document will be reviewed by the Caldicott and Information Governance Assurance Committee and ratified by the Director of Corporate Business.

Non-significant amendments to this document may be made, under delegated authority from the Director of Corporate Business, by the nominated author. These must be ratified by the Director of Corporate Business and should be reported, retrospectively, to the Caldicott and Information Governance Assurance Committee.

Significant reviews and revisions to this document will include a consultation with named groups, or grades across the Trust. For non-significant amendments, informal consultation will be restricted to named groups, or grades who are directly affected by the proposed changes.

7 | Dissemination and Implementation

Following approval and ratification, this procedural document will be published in the Trust's formal documents library and all staff will be notified through the Trust's normal notification process, currently the 'Vital Signs' electronic newsletter.

Document control arrangements will be in accordance with The Development and Management of Formal Documents.

The document author(s) will be responsible for agreeing the training requirements associated with the newly ratified document with the Director of Corporate Business and for working with the Trust's training function, if required, to arrange for the required training to be delivered.

8 | Monitoring and Assurance

The Information Governance team will obtain a list of staff who have requested a key and the reason why from the parking desk on a monthly basis to cross reference with Datix.

Staff that repeatedly request a key will be contacted by the Information Governance team to investigate further.