



“An Excellent Authority”

APPENDIX E

Service Instruction 0759

Destruction of Information Assets (Including Protectively Marked Information)

Document Control

Description and Purpose

This instruction is intended to provide guidance to all MFRS personnel about the destruction of Information Assets including Home Fire Safety Check Case Files

Active date	Review date	Author	Editor	Publisher
11/05/2012	01/11/2014	Jean Crimmins	Deb Appleton	Sue Coker
Permanent	<input checked="" type="checkbox"/>	Temporary	If temporary, review date must be 3 months or less.	

Amendment History

Version	Date	Reasons for Change	Amended by
2	03/09/2013	Content of the SI amended (SI 0675, SI0146 and SI 0759 now merged as one instruction) Also included a section on the destruction of Archived paper records held in Vesty Stores	Jean Crimmins

Risk Assessment (if applicable)

Date Completed	Review Date	Assessed by	Document location	Verified by(H&S)

Equalities Impact Assessment

Initial	Full	Date	Reviewed by	Document location

Civil Contingencies Impact Assessment (if applicable)

Date	Assessed by	Document location

Related Documents

Doc. Type	Ref. No.	Title	Document location
Service Instruction	0438	Data Protection Instructions	Portal
Service Instruction	0400	Waste Management and Minimisation	Portal
Service Instruction	0433	Retention of Records	Portal
Policy	KIMPOL09	Information Governance and Security Policy	Portal

Contact

Department	Email	Telephone ext.
Strategy and Performance	strategyandperformance@merseyfire.gov.uk	4474/4479

Target audience

All MFS	<input checked="" type="checkbox"/>	Ops Crews	<input type="checkbox"/>	Fire safety	<input type="checkbox"/>	Community FS	<input type="checkbox"/>	<input type="checkbox"/>
---------	-------------------------------------	-----------	--------------------------	-------------	--------------------------	--------------	--------------------------	--------------------------

Principal officers		Senior officers		Non uniformed				
---------------------------	--	------------------------	--	----------------------	--	--	--	--

Relevant legislation (if any)

Data Protection Act 1998.
Freedom of Information Act 2000.
Lord Chancellor's Code of Practice on the management of records issued under section 46 of the Freedom of Information Act 2000.
Environmental Permitting Regulations 2010
Environmental Protection (Duty of Care Regulations) 1991

Instruction

HANDLING AND DESTRUCTION OF INFORMATION ASSETS (INCLUDING PROTECTIVELY MARKED INFORMATION)

1. Introduction

Information and data are necessary for Merseyside Fire and Rescue Authority (MFRA) to arrange and provide services for the citizens of Merseyside. All Members, employees, contract and temporary workers have a responsibility to ensure that information and data are securely disposed of when they are no longer required in order to safeguard from inappropriate release, modification or misuse. Information and the way it is used, processed, stored and eventually disposed of, is subject to legislation and regulation. Information assets may be produced on a daily basis, and can include printed material as well as handwritten information.

Prior to undertaking manual handling in the preparation of Information Assets waste material, please ensure you read and understand Service Instruction [SI 0021 Manual Handling](#).

2. Objective

The objective of this service instruction is to

- Protect MFRA's information from all threats (whether internal or external, deliberate or accidental);
- To ensure business continuity, minimise damage and maximise our ability to deliver services.
- To protect data owned by MFRA;
- To protect the identity of MFRA staff and service users;
- To demonstrate compliance with legal obligations around protected data.

This service instruction governs the disposal of any waste material that contains information that would constitute a breach of confidentiality if it became available to unauthorised persons and applies to ALL MFRA staff and locations.

3. Scope

The scope of this service instruction is to provide advice and guidance to MFRA on:

- How to identify Information Assets waste;
- How to store Information Assets waste;
- How to dispose of Information Assets waste.

4. How to identify Information Assets waste

Information Assets waste is material which has any of the following characteristics:

- Material that contains information that would identify an individual person or employee or contains business sensitive information. This applies to all materials regardless for format, e.g. paper, video or audiotape, DVD, photograph, disk, external drive etc.

Service Instruction 0759: Destruction of Information Assets (Including Protectively Marked Information)

- Records containing personal information e.g. completed HFSC forms, payroll and pensions' records and staff files.
- The Data Protection Act 1998 distinguishes between "ordinary personal data" such as name, address and telephone number and "sensitive personal data" including information relating to racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sex life and criminal convictions. Under the Act the processing of sensitive data is subject to much stricter conditions.
- Records of a commercially sensitive nature e.g. contracts, tenders, purchasing and maintenance records and legal documents.
- Records concerning intellectual property rights e.g. unpublished Service Instructions and Policy documents, training documents.
- Authority reports and other documents marked as "exempt – not for publication".
- Any other organisationally sensitive material not in the public domain (at the time of it being discarded) that has been produced by MFRA or its partners.
- Specific instructions relating to Home Fire Safety Check Case Files are included at Appendix 1.
- Documents marked with the Government Protective Markings PROTECT, RESTRICTED, CONFIDENTIAL, SECRET AND TOP SECRET

5. Handling Information Assets waste

Information Assets waste must be kept secure and protected against accidental loss, damage or unauthorised access up until it is processed for destruction.

- Information Assets waste **MUST NOT** be placed in the recycling bins/green recycling bags unless it has been shredded first. A poster that explains this is attached at Appendix 2. This should be printed off and attached to each recycling box.
- Unshredded Information Assets waste should be kept separate from other waste material e.g. wastepaper bins, recyclable material.
- Unshredded Information Assets waste awaiting collection must be kept secure at all times.
- Remove non paper based containers e.g. lever arch files, plastic folders, ring binders, plastic covers etc. It may be possible to reuse or recycle some of this material.
- Non paper based material e.g. videos or audiotapes, DVDs, disks, external drives etc. **must be separated** from paper based records.
- External drives must be returned to ICT/telent for disposal.
- Some non-paper based material can be destroyed by shredding e.g. DVDs and CDs. This method would be suitable for small quantities. Contact the Records Management Team for further information: recordsmanagement@merseyfire.gov.uk
- Records that have been identified for destruction that are required for litigation, Freedom of Information (FOI) requests, Data Protection Act (DPA) subject access requests, inquiries, investigations, litigation etc., **must be placed on "hold" and not removed for destruction.**

6. How to dispose of Information Assets waste

Information Assets Waste **MUST** be destroyed in one of 2 ways:

- Shredding by a member of MFRA staff;
- Contracted to an approved confidential waste service provider for shredding and disposal.

6.1 Shredding by a member of MFRS staff

This option should be used for small to medium volume of Information Assets waste, anything from one sheet of paper to between 2-4 filing cabinet drawers or shelves. Shredding is an acceptable method of total destruction of Information Assets and the remains are safe to be sent for recycling. Simple vertical shredding is not suitable for personal and protectively marked information and a cross cutting shredder must be used to shred the information. Shredders are accessible at SHQ and on all Stations. If you do not have access to a shredder, please contact the Procurement Team via email: Procurement@merseyfire.gov.uk. The Procurement Team will be able to arrange access to the SHQ high capacity shredder or arrange for repair or replacement of Station based shredders.

Protectively Marked Information

- PROTECT and RESTRICTED: Use a cross cut shredder or put your documents in a confidential waste sack that is collected by an approved waste collector. This will make it unlikely that anyone will be able to read the information.
 - CONFIDENTIAL: Tear up documents and place them in a confidential waste sack that is collected by an approved waste collector. Alternatively, shred as SECRET.
 - SECRET: The documents should be shredded in a cross cutter; put the paper in at right angles to the print. The size of the shredded strips should be no more than 0.8mm and 12mm and not show more than two characters side by side. This will make it highly unlikely that anyone can put the document back together. When destroying SECRET documents, a record must be retained of the date the document was destroyed and who authorised its destruction. This record must be kept for five years.
 - TOP SECRET: These documents must be destroyed in the same way as SECRET documents, except that two people must witness the shredding and sign the registry.
-
- Follow guidance provided in section 5 to prepare Information Assets waste for shredding;
 - Once the material has been shredded it **MUST** be transferred to recycling bags;
 - Contact Estates team: Estates@merseyfire.gov.uk, to request appropriate bags for the recycling of shredded waste.
 - Cleaning staff will transfer recycling bags to the paper recycling wheelie bins in SHQ Waste Management Yard.
 - ***For staff NOT based at SHQ please give bagged, shredded waste to the Tender drivers who will arrange to transfer it to SHQ and place the bags in the recycling wheelie bins in SHQ Management Yard. Do not place shredded paper in the local authority recycling bins.***
 - It is an offence to allow waste to escape, so bags of shredded paper must be tied and placed within a secure area (e.g. wheelie bin, cage etc.) until they are collected for destruction.

6.2 Outsourced to an approved confidential waste service provider

This option can be used for large volume of Information Assets waste, for example, in excess of 2-4 filing cabinet drawers or shelves. This option incurs a cost and you must ensure you have sufficient budget to cover the cost of processing the waste. To assist in making the decision about which option to use please contact the records management team who will be able to provide an approximate cost for the work recordsmanagement@merseyfire.gov.uk.

7. Process

7.1 Ordering Information Assets waste bags

Please state type of Information Assets waste; either paper based or non-paper based (e.g. DVDs, discs) and the number of bags you require. To obtain Information Assets waste bags, contact:

- Julie Yare/Jean Crimmins – Corporate Information Sharing Team based at Service Headquarters. Contact details are:
- Email: julieyare@merseyfire.gov.uk or jeancrimmins@merseyfire.gov.uk
- Telephone: 0151 296 4479 / 4474

7.2 Information Assets waste preparation

The following process must be completed to prepare Information Assets waste for collection:

- Information Assets waste should be removed from non-paper based containers e.g. lever arch files, plastic folders, ring binders, plastic covers etc.
- Information Assets waste must be placed in bags provided. It is important not to over fill or under fill each bag. Each bag will hold up to a maximum of 17kg, capacity is clearly marked on the bag.
- Removal of bulldog clips, staples or paper clips from Information Assets waste is not required.
- Non paper based material e.g. videos or audiotapes, DVDs, photographs, disks, external drives etc. **must be separated** from paper records and placed in bags that are specifically for non-paper based waste.
- Records that have been identified for destruction that are required for litigation, FOI requests, DPA requests, inquiries etc., must be placed on “hold” and not removed for destruction.
- When the Information Assets waste is ready complete a Waste Information Collection Form (See Appendix 3 for an example of the form). The form must be emailed to Julie Yare / Jean Crimmins. The form is available from the Records Management page on the Portal.

7.3 Information Assets waste collection

You will be notified of the collection day in advance and by no less than 5 working days prior to collection. All bags of Information Assets waste should be stored in a secure area until the collection day. A representative from each team/department should be available on the day to oversee the Information Assets waste collection. A certificate of destruction will be obtained from the waste contractor and retained for not less than 2 years from the date of collection.

8. Process for Destruction of Archived Paper Records Held in Vesty Stores (Archive Area)

- The existing Records Database (located on the Portal) indicates when records are due for review or destruction.
- The Corporate Information Sharing Officer will e-mail the Record owner with a list of those records that need to be reviewed or destroyed.
- The Record owner will then confirm to the Corporate Information Sharing Officer that the records are authorised for destruction or if a further retention period needs to be applied.
- The Record owner or designated member of staff will then complete the RM database request form so that the relevant boxes can be removed from the Archive area in readiness for destruction. It is the responsibility of the Record owner (or delegated person) to remove the records from the boxes and place into Information Assets waste bags. **THIS WILL NOT BE ACTIONED BY STORES STAFF.**
- The Records must then be destroyed using an approved Information Assets Waste provider (See Section 6.2 and Section 7 of this Service Instruction)

Related Policies and Service Instructions:

STRPOL09 Information Governance & Security Policy.

SI 0437 Freedom of Information requests and Publication Scheme

SI xxxx CCTV Use

SI 0759 Destruction of Information Assets (including protectively marked document)

SI 0687 Preparing & Transferring Records to Storage in RM Archive Store Vesty Building.

ICTPOL03 Acceptable use policy

SI0703 Internet Access and Usage

SI0699 Using Social Media

SI0730 Email

STRPOL (to be agreed) – Protective Security Policy – in draft

Protective Marking SI in draft

Personal Security SI in draft

Appendix 1

HOME FIRE SAFETY CHECK (HFSC) CASE FILES HELD ON DISTRICT STATION

GUIDANCE

- Home Fire Safety Check (HFSC) paper form is completed by staff member (Prevention Advocate or Fire Support Network Volunteer)
- A duplicate copy of the HFSC form is kept in the Prevention Office and the original is sent to Fire Service Direct.
Fire Service Direct then confirm receipt of the forms and also confirm entry onto the database (confirmed in both instances by e-mail, within a 48 hour period).
- Any case files that include any outside agency involvement must be kept for 5years, due to the nature and content of the file. i.e. Social Services, GP.

ARCHIVED CASE FILES HELD ON DISTRICT STATION

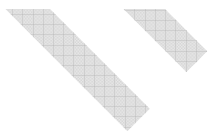
It was agreed on 14/05/09 that all paper case files must be kept for 5 years and then annually on 1st April the case files that are over 5 years old must be disposed of in line with the requirements set out elsewhere in this Service Instruction

Help and further assistance

Contact:

Prevention and Protection
Service Headquarters 0151 296 4000

Corporate Information Sharing Officer
Service Headquarters 0151 296 4000



Appendix 2

Information Assets waste poster

Appendix 2 contains an Information Assets Waste poster that **MUST** be displayed on existing Energy wise or EWR recycling bins. For locations that do not have an Energy wise or EWR recycling bin, the poster **MUST** be displayed in the Station Office and/or the Watch Manager's office.

Instruction

INFORMATION ASSETS WASTE

DO NOT PLACE UNSHREDDDED ITEMS IN A RECYLCING BIN IF THEY CONTAIN:

- **PERSONAL INFORMATION – E.G. NAMES AND ADDRESSES, DATE OF BIRTH.**
- **PROTECTIVELY MARKED INFORMATION – ie Marked “PROTECT”, “RESTRICTED”, “CONFIDENTIAL”, “SECRET”, “TOP SECRET”**
- **COMMERCIALLY SENSITIVE INFORMATION – CONTRACTS, TENDERS, LEGAL DOCUMENTS.**
- **ORGANISATIONALLY SENSITIVE INFORMATION NOT YET IN THE PUBLIC DOMAIN - E.G. DRAFT REPORTS, DRAFT LETTERS, INCLUDING HANDWRITTEN MATERIAL.**
- **INTELLECTUAL PROPERTY RIGHTS – E.G. UNPUBLISHED SERVICE INSTRUCTIONS, POLICY, TRAINING DOCUMENTS.**
- **EXEMPT AUTHORITY REPORTS AND OTHER EXEMPT DOCUMENTATION.**

Please see SI 0759 – Destruction of Information Assets Waste (Including Protectively Marked Information) for further guidance.

PLEASE DIRECT ANY QUERIES TO THE RECORDS MANAGEMENT TEAM:
RECORDSMANGEMENT@MERSEYFIRE.GOV.UK

Appendix 3

Complete PART A – items 1 – 4

1. Your details	
Directorate:	
Your Details	
Team name:	
Your Role/ Job Title	
Your name:	
Your Service Number	
Today's date:	

2. Information Assets waste	
Number of bags of paper based confidential waste ready for collection:	
Number of bags of non-paper based confidential waste ready for collection:	
Location of bags. Please indicate building and room number, cage number etc. :	

3. Information Assets waste contents		
Please provide details of items destroyed including series name and date range . For example: Home Fire Safety Checks, 01/01/2004 -31/12/2004. Please do not record business sensitive or personal information on this form.		
Series description	Date range	Waste tag serial nos.
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		

(Continue on a separate sheet if necessary)

4. Waste checklist		Please tick to confirm
1.	All waste has been placed in appropriate bags.	<input type="checkbox"/>
2.	Non paper based material e.g. videos or audiotapes, DVDs, photographs, disks, external drives etc. have been separated from paper records and placed in special bags that are specifically for non-paper based waste.	<input type="checkbox"/>
3.	The records are NOT required for litigation, FOI requests, DPA requests, and audits at this time.	<input type="checkbox"/>
4.	Business Sensitive and Personal Information waste is stored in a secure, locked area whilst waiting for collection.	<input type="checkbox"/>

Information Assets waste will not be collected unless this form is completed

Part B. Do not use			
5. Office use only			
5.1	All sections completed:		
5.2	Returned to requestor to complete in full the following sections:		
5.3	Number and type of bags collected:	Paper based:	Non paper based: Date:
5.4	Budget code:		
5.5	Date authorised :		
5.6	Waste certificate obtained, ref no and date:		
5.7	Security tag serial no:		

Instruction