Merseyside FIRE & RESCUE SERVICE

"An Excellent Authority"

SERVICE INSTRUCTION 0435
DATA PROTECTION INSTRUCTIONS

Document Control

Description and Purpose

This document is intended to give guidance to all MFRS personnel about the Data Protection Act 1998 and processing personal data.

Active date	Review date	Author	Editor	Publisher
27/11/08	01/11/2014	J.Yare	D. Appleton	Sue Coker

Permanent	×	Temporary		If temporary, review date must be 3 months or less.

Amendment History

Version	Date	Reasons for Change - update	Amended by
2	16/10/2014	Update and to tie in with other policies and SI's	J. Yare

Risk Assessment (if applicable)

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

Equalities Impact Assessment

Initial	Full	Date	Reviewed by	Document location
N/A	N/A	N/A	N/A	N/A

Civil Contingencies Impact Assessment (if applicable)

Date	Assessed by	Document location
N/A	N/A	N/A

Related Documents

Doc. Type	Ref. No.	Title	Document location
Old SOP	ADM0041		Document Archived
Policy	STRPOL09	Information Governance & Security	Portal
Service Instruction	SI 0437	Freedom of information	Portal
Service Instruction	SI0725	Close Circuit Television	Portal
Service Instruction	SI	Destruction of information Assets (Including Protectively Marked Information)	Portal
Service	SI	Service Leavers	Portal

Instruction			
Service Instructions	**ICTPOL03**	**Acceptable Use Policy**	**Portal**
Service Instruction	**SI 0703**	**Internet Access and Usage**	**Portal**
Service Instruction	**SI 0699**	**Using Social Media**	**Portal**
Service Instruction	**SI 0730**	**Email**	**Portal**

Contact

Department	Email	Telephone ext.
Strategy & Performance	**jeancrimmins@merseyfire.gov.uk** **julieyare@merseyfire.gov.uk**	**4474/4479**

Target audience

All MFS		**Ops Crews**		**Fire safety**		**Community FS**			
Principal officers		**Senior officers**		**Non uniformed**					

Relevant legislation (if any)

Data Protection Act 1998
Common Law Duty of Confidentiality
Common Law Duty of Confidence

DATA PROTECTION

Table of Contents

1. Introduction

The Data Protection Act 1998 also supports the Fire and Rescue Service Protective Security Strategy which will ensure that access to information is correctly managed and safeguarded to an agreed and proportionate level throughout the information lifecycle, including creation, storage, transmission and destruction.
It is the aim of MFRA that all appropriate staff are properly trained, fully informed of their obligations under the Data Protection Act 1998 and are aware of their personal liabilities.

Any employee acting outside the requirements of the Authority's Data Protection Instructions will be subject to MFRA's disciplinary procedures, and possible legal action. Individuals whose information is held and processed by MFRA can be assured that MFRA will treat their personal data with all due care. It is possible that at times disclosures of information may be made through other legislation or through the non-disclosure provisions/exemptions of Data Protection law.

The Authority's Senior Information Risk Owner (SIRO), with the support of the Information Security Forum is responsible for ensuring that the overall Information Security and Governance Policy is adhered to and that it reflects the information security needs of MFRA.

This document explains how Merseyside Fire & Rescue Authority (MF&RA) will meet the legal requirements of the Data Protection Act 1998. The Data Protection Act 1998 established a framework of rights and duties which are designed to safeguard personal data. This framework balances the legitimate needs of organisations to collect and use personal data for business and other purposes against the right of individuals to respect for the privacy of their personal details.

The Act extended the rights given to individuals in previous legislation and requires data controllers (people or organisations that hold and process details of living individuals) to comply with the Eight Principles (rules governing the use of personal data). Also they must bear in mind the rights and freedoms of those individuals when processing their details.

2. The Eight Principles

- Personal data shall be processed fairly and lawfully.
- Personal data shall only be obtained for specified and lawful purposes, and shall not be processed for any other incompatible purpose
- Personal data obtained shall be adequate, relevant and not excessive.
- Personal Data should be accurate
- Personal data shall not be kept any longer than necessary.
- Personal data shall be processed in accordance with the rights of the data subject.
- Appropriate measures shall be taken against unauthorised or unlawful processing of data, and against accidental loss or destruction of, or damage to, personal data.
- Personal data shall not be transferred outside the European Economic Area (EEA) unless adequate protection is afforded to the rights and freedoms of the data subject.

3. Fair Obtaining/Processing

MFRA will, as far as it is practicable, ensure that all individuals whose details we hold are aware of the way in which that information will be held, used and disclosed. Individuals will, where possible, be informed of the likely recipients of the information – whether the recipients are internal or external to MFRA. Processing within MFRA will be fair and lawful, individuals will not be misled as to the uses to which MFRA will put the information given. If a person feels they have been deceived or misled as to the reason for which their information was collected, they should use the MFRA'

Collection forms requiring personal information will contain a 'fair processing' statement giving details of the likely uses of the information, where information is collected in person or by telephone the employee asking for the details will tell the individual how those details will be used. People are free to ask the person collecting the information why they want the details and what they will be used for.

Example of 'Fair Processing' Statement

"The information you have provided will be held by Merseyside Fire and Rescue Authority for the purposes of processing and administration and will be added to your personal file. Please notify us immediately of any changes so that we can keep your information up to date. Personal data may be disclosed to the data subject, data processors and Personnel staff. Occasionally we may be required by legislation to disclose data to Government Agencies".

If a person's details are going to be used for 'auto decision' processing (where a computer or other process decides something based on a score or other information) the person will be told about how the system works and whether the decision can be challenged.

If a person's details are to be processed for a purpose that does not appear on MFRA's notification submitted to the Information Commissioner, the individual will be given the information that would be necessary to make the processing fair and lawful.

Any person whose details are to be included in the organisation's website will be asked to give written consent. At the time the information is inserted, all such individuals will be properly informed about the consequences of their data being disseminated worldwide.

For further information on the processing of personal data please refer to guidance on the portal at http://intranetportal/sites/kim/InformationGovernance/default.aspxor go to the Information Commissioners website www.ico.gov.uk.

4. Data Uses and Processes

MFRA will not use or process personal information in any way that contravenes its notified purposes or in any way that would constitute a breach of Data Protection Law. Any new purposes introduced will, where appropriate, be notified to the individual and - if required by the law – their consent will be sought. A copy of the appropriate notification document is available from MFRA's Corporate Information Sharing Officer (CISO). The notification document can also be viewed on the Information Commissioner's web page www.ico.gov.uk registration no Z4919035

MFRA has a reporting structure headed by the Senior Information Risk Owner (SIRO), with an Information Asset Owner (please see Appendix 1) (IAO), in each department to ensure the following:

- all purposes and disclosures are co-ordinated and consistent
- all new purposes are documented and notified to the Information Commissioner
- all problems can be investigated thoroughly
- the SIRO and/or the Service CISO is informed of all new databases or other IT systems using or processing personal data to ensure the specification and the chosen system database addresses the principles of Data Protection.

5. Data Quality and Integrity

MFRA will not collect data from individuals where that information is excessive or irrelevant in relation to the notified purpose(s). Details collected will be adequate for the purpose and no more. Information collected which becomes (over time or by virtue of changed purposes) irrelevant or excessive will be deleted. Staff responsible for particular data sets will take on the role of IAO as previously mentioned (List at Appendix 1), and with it the responsibility for working with the SIRO to implement best practice and reduce risk to personal data.

MFRA will ensure, as far as it is practicable, that the information held is accurate and up to date. It is the intention of MFRA to check wherever possible the details given. Information received from third parties will carry a marker indicating the source. Where a person informs MFRA of a change of their own circumstances, such as home address or non-contentious data, their record(s) will be updated as soon as possible. Where the individual requests that information be changed and it is not possible to update it immediately, or where the new information needs to be checked for its accuracy or validity, a marker will be placed on the disputed record indicating the nature of the problem.

MFRA and the individual will attempt to reach an amicable agreement on the dispute but where this is not possible MFRA's grievance or complaints procedures will be implemented.

6. Retention of Records

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. In practice, it means that the person responsible for the data will need to:

- Review the length of time personal data is kept by working with the CISO to set a retention schedule.
- Consider the purpose or purposes for which the information is held in deciding whether (and for how long) to retain it;
- Securely dispose of or delete information that is no longer needed for this purpose or these purposes; and
- Update, archive or securely dispose of or delete information if it goes out of date.

Where details of individuals are stored for long-term archive or historical reasons and where it is necessary to retain the personal detail within the records it will always be done within the requirements of the legislation. In many cases personal details will be removed from the record so that individuals cannot be identified. For individual retention schedules please refer to the portal on http://intranetportal/sites/kim/recordsmanagement/Pages/ArchivedRecords.aspx or Contact the CISO. Also see SI 0687 for more details on Preparing and Transferring records to the Records Management Archive Store/Vesty Building.

Redundant personal data will be destroyed in accordance with the Data Protection Act. For more information on the disposal of personal data please refer to SI 0759 Destruction of Assets (including Protectively Marked Information), on the Portal.

In general, paper waste is shredded by each individual department or destroyed by a professional records management company. Magnetic media (disks, tapes, etc.) must be physically destroyed beyond recovery.

7. Subject Access Requests

Any person whose details are processed by MFRA has a general right to receive a copy of their own information. Individuals will be able to have a copy of the data held on them. MFRA has a policy of charging £10 for such requests in line with the guidance of the Information Commissioner. Any codes used in the record will be fully explained and any inaccurate, out of date, irrelevant or excessive data will be dealt with under the procedures outlined in 'Data Quality & Integrity'.

MFRA will attempt to reply to subject access requests as quickly as possible and in all cases within the 40 days allowed by the Data Protection Act. Repeat requests will be fulfilled unless the period between requests is deemed unreasonable, such as a second request received so soon after the first that it would be impossible for the details to have changed.

A subject access/information request should be submitted on the appropriate forms wherever possible. This will ensure that MFRA has the required information to be able to conduct a data search and to fulfill the request. In some cases, especially with requests not submitted on the correct form, further information may be required from the requester which may delay the start of the 40-day maximum time limit.

Subject Access Request forms are available from the CISO or on the portal at http://intranetportal/sites/kim/InformationGovernance/default.aspx

8. Technical and Organisational Security

MFRA has implemented appropriate security measures as required under the Data Protection Act 1998. In particular, unauthorised staff and other individuals are prevented from gaining access to personal information. Appropriate physical activity is in place with visitors being received and supervised within MFRA offices where information about individuals is stored. The general public visiting MFRA offices should not feel that the measures are restrictive or oppressive. The measures are there to protect MFRA's data and other assets.

Computer systems are installed with user-profile type password controls and, where necessary, employee and access trail to establish that each user is fully authorised. In addition, employees are fully informed about overall security procedures and the importance of their role within those procedures. All employees of MFRA are required to save data to their designated network drives and not to their individual PC's in line with principle 7 of the Data Protection Act 1998.

Manual filing systems are held in secure locations and are accessed on a need-to-know basis only. Records and documents containing personal data must always be secured in a locked room, drawer or cabinet when not being worked on.

MFRA policies on the use of e-mail and internet facilities will also have an impact on technical and organisational security; refer to STRPOL09 Information Governance & Security Policy and associated ICT policies and SIs.

9. Portable storage devices

Storing Personal Data on portable devices e.g. lap tops, portable hard drives; CDs, DVDs and memory sticks should always be avoided. However, if this is essential for organisational reasons, such devices should always be encrypted and/or password protected.

Staff, volunteers and where relevant, Elected Members and contractors must order encrypted devices through the telent ICT request forms.

10. Disclosures of Information under Section 29 and Information Sharing

It is sometimes necessary to disclose or share personal data and this is possible within the Data Protection Act. All staff are informed and reminded about the limits of their authority on disclosing information both inside and outside MFRA.

Disclosure on an adhoc basis - personal data on individuals will only be disclosed on a need to know basis inside and outside MFRA. Where details need to be passed outside the organisation it will, in general be done for an already registerable purpose, with the person's consent or through an exemption under the Act. An example of this would be the Police requesting information under Section 29 - Crime & Taxation. A request for disclosure form would always be required from an outside organisation before disclosure was permitted for MFRA's audit trail. When requesting information from other organisations MFRA staff are required to use the disclosure form available on the Portal at http://intranetportal/sites/kim/InformationGovernance/default.aspx

Information Sharing usually involves sharing bulk data, about many individuals on a regular basis. An example is an Information Sharing Protocol with a local authority, where the local authority provides MFRA with benefits data for prevention purposes with specified field's e.g. name, address, telephone no, postcode and D.O.B.

MFRA use Information Sharing Protocols, as recommended by the Information Commissioner's Office, to agree terms that ensures that all sharing meets the requirements under the Data Protection Act 1998. The protocols set out the organisations involved, the reason for sharing, and the data fields to be shared, frequency of sharing, the secure system that is to be used and the legislation that the information is being shared under. For advice on Information Sharing contact The CISO.

It is a specific requirement of the Data Protection Act that personal data is not transferred outside the European Economic Area (EEA) without assured safeguards being met or without the individual's consent. Accordingly personnel are instructed to ensure that data is only transferred outside the EEA following consultation with the CISO.

11. Reporting the loss of Personal Data

Any member of staff, Authority Member, volunteer or contract worker who thinks they may have lost, had stolen or mistakenly disclosed personal data belonging to MFRA, either in hard copy or electronic form should take the following action as soon as possible after they discover the loss;

- Inform their line manager of the data loss and the circumstances that led to it
- Email dataprotection@merseyfire.gov.uk with the same details or ring the CISO on 0151 296 4479 or 4479 and
- Where the data was held on an electronic device; contact the telent helpdesk to inform them of the loss
- Where the data and/or the device on which it was stored have been stolen; report the theft to the Police

All reported breaches or potential weaknesses are investigated and, where necessary, further or alternative measures will be introduced to secure data. Such reports will be received by the SIRO, the appropriate department head as necessary and in some cases, disciplinary action could be taken.

Security arrangements are reviewed regularly. For further information on Information Security please refer to the Information Governance section located on the Portal or STRP0L09, the Information Governance and Security Policy.

12. Data Processors

MFRA will use third parties to carry out various services to allow the Service to work efficiently. The third party will act as a 'data processor' on MFRA's behalf. Where any third party processing takes place there must be a written contract between MFRA and the data processor. In the contract MFRA will oblige the processor to take measures in respect of the personal data processing as would comply with the requirements of the Data Protection Act 1998. In every case, MFRA will take steps to ensure satisfaction that the processor is complying with this contractual obligation. All data processors for MFRA will be given a current copy of its Data Protection Instructions S.I.

Further Information, Enquiries and Complaints

MFRA's CISO and the SIRO are the first point of contact on any of the issues mentioned in this service instruction. The SIRO and the CISO will be responsible for dealing with all internal and external enquiries and where possible, requests for detailed information should be in writing.
MFRA will attempt to complete internal investigations into any complaint within 28 days and in every case the person will receive an acknowledgement within 2 working days after receipt of the complaint.

Contact Details

The CISO is based at Service Headquarters – 0151 296 4474/4479. For details of IAO please see Appendix 1...

This service instruction is also linked to the following policies and service instructions.

STRPOL09 Information Governance & Security Policy.
SI 0437 Freedom of Information requests and Publication Scheme
SI 0725 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

Function/ directorate	Data Manager	Location	Contact Extension No.	System
Assets	Stewart Woods	Estates	EXTN 4514	Word/ Excel
Assets	Jimmy Brannan	Transport	EXTN 4548	Sophtlogic
Corporate Communications	Peter Rushton	Corporate Communication	EXTN 4557	
Finance	Mike Rea	Finance	EXTN 4202	FMIS
Legal and Democratic Services	Sarah Bourne	Legal Services	EXTN 6212	N/A
Operational Response	John McNeill	Health and Safety	EXTN 4362	OSHENS
Operational Response	Mike Pilkington	Time and Resource Management	EXTN 4303	HR system
Operational Preparedness	Cathy Scarth,	Data Management	EXTN 4478	VISION IRS
Operational Preparedness	Ged Sheridan	TDA	EXTN 5022	HR System SPA system
Operational Preparedness	Jim Martin	Appliances/Equip ment	EXTN 4534	REDKITE
Operational Preparedness	Jackie Gleaves	Water Section	EXTN 4511	Infoterra Hydrant Management
People and Organisational Development	Paul Blanchard-Flett	Occupational Health	EXTN 4339	HR System
People and Organisational Development	Suzanne Lea	People Data	EXTN 4320	HR System
People and Organisational Development	Phil Dwyer	Pay and Pensions	EXTN 4219	Professional Standards
People and Organisational Development	John Price	Learning and Development	EXTN 4317	HR System
Prevention and Protection	Caroline Crichton Guy Keen Kevin Johnson Karen Metcalf	Community Prevention and Protection	EXTN 4601	Capita Protection System Goldmine Children and Young People
Procurement	Sharon Matthews	Procurement	EXTN 4556	E-Procurement
Principal Officers	Sandra Wainwright Lin Morrison Nyree Collinson	Principal Officers Suite	EXTN 4102	N/A
Strategy and Performance	Paul Terry,	Systems Support	EXTN 4402	VISION MapInfo Portal SinglePoint
Strategy and Performance	Wendy Kenyon	Diversity Team	EXTN 4564	
Technology	Mark Hulme	ICT	EXTN 4569	Overall Applications Management

APPENDIX 2

Glossary of Terms

Data

"Data" means information:

- Stored in a form capable of being processed by computer or other automatic equipment (such as most computer files, including word processor, database and spreadsheet files)
- Recorded in any form for later processing by computer or other automatic equipment (such as information collected from registration forms; CCTV pictures)
- Stored as part of a relevant filing system or intended to be included in one in the future (including card files or filing cabinets structured by name, address or other identifier; Rolodex; non-automated microfiche)

Personal Data

"Personal data" are data which relate to a living individual who can be identified from that information, or from that data and other information in the possession of the data controller or which are likely to come into his or her possession. These include any expression of opinion about the individual and of the intentions of the data controller in respect of that individual.

Sensitive Personal Data

The 1998 Act 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.

Data Subject

A "data subject" is any living individual who is the subject of personal data.

Data Subject Access

"Data subject access" is the right of an individual to access personal data relating to him or her which is held by a data controller.

Data controller

A "data controller" is the nominated person in an organisation who makes decisions with regard to particular personal data, including decisions about the purposes for which the personal data are processed and the way in which the personal data are processed.

Data processor

A "data processor" is a person who processes the data on behalf of the data controller, but who is not an employee of the data controller.

Processing

The definition of "processing" is no longer confined to technical processing operations on data, such as organisation, retrieval, disclosure, and deletion; it also includes:

- Obtaining and recording data
- The retrieval, consultation or use of data
- The disclosure or otherwise making available of data

Information Sharing plays an important part in the role of CISO working with uniformed members of staff and the Project Manager for the Customer Insight Project, to build relationships with other organisations and highlight the most vulnerable members of the community. This enables MFRA to provide a Home Fire Safety Check to people who need it most and in many cases vital contact with other support agencies.

MFRA has Information Sharing Agreements in place with many partner organisations where these partners hold data that will assist MFRA target vulnerable people examples of these agreements are held on the Portal under Strategic Planning/Knowledge & Management/ Information Governance/Information Sharing.

Sharing personal data with partner organisations is vital to ensuring MFRA continues to target prevention interventions effectively. When approaching external organisations to ask if they would be willing to share personal data with MFRA can you please ensure that your staff are aware of the following process:

- If a meeting is arranged with an organisation please invite the Corporate Information Sharing Officer (CISO) to the meeting.
- At the meeting the CISO will explain that AVCO should be used to transfer the data to MFRA. AVCO is a secure, encrypted way of transferring data with no cost to the external organisation. Also, a specific Data Template is used and this ensures that the data can be matched with our Goldmine database.
- An Information Sharing Protocol should also be set up. MFRA has a template that can be used if the organisation does not have their own and the CISO will liaise with the organisation to advise and draft and complete the protocol.

This will help the organisations that are willing to share information (and MFRA) protect individuals' personal data and demonstrate that MFRA is an organisation that takes information security and data protection seriously.

Records Management, including retention, archiving and destruction of confidential and non-confidential waste are also relevant to the successful handling of personal data.

The Information Security Forum

All matters relating to Information Security including Data Protection are monitored and managed by the MFRA Information Security Forum, chaired by the SIRO to maintain good Information Security.