APPENDIX A

Service Policy No. STRPOL09 Information Governance & Security Policy

Document Control

Active date	Review date	Department	Author	Editor	Publisher
	April 2014	Strategy & Performance	Julie Yare	Information Security Forum (ISF)	Sue Coker

Legislation

Title		
	Data Protection Act 1998 **Freedom of Information Act 2000** **Protection of Freedoms Act 2012**	

Amendment History

Version	Date	Author	Reasons for Change
3	October 13	Julie Yare	Combined Information Governance, Data Protection & Security Policy.

Amendment History

Version	Date	Author	Reasons for Change
1	October 13	Julie Yare	Combined Information Governance, Data Protection & Security Policy.

Equalities Impact Assessment

Initial	Full	Date	Reviewed by	Comments
X		**09.05.07**		
JY	YES	July 2013	Wendy Kenyon	

Civil Contingencies Impact Assessment

Date	Reviewed by	Comments

Related Policies

Title	Author	Department

Distribution List

Name	Position	I/R
Information Security Forum		I
Senior Management Group		R

Sign-Off List

Name	Position
Information Security Forum	
Senior Management Group	

Related Documents

Ref No.	Title	Author	Version & Date
SI 0435	Data Protection Instructions	J. Crimmins	
SI 0437	Freedom of Information Requests/Publication Scheme	J. Crimmins	
SI xxxx	CCTV	G. Davies	
SI 0759	Destruction of Information Assets (including Protectively Marked Information)	J. Crimmins	
SI 0687	Preparing and transferring records to storage in the Archive Store, Vesty building	J. Crimmins	
ICTPOL03	Acceptable use policy	Bernie Kenny	
SI0730	Internet Access & Usage	Bernie Kenny	
SI0703	Email	Ed Franklin	
SI0699	Using Social Media	Bernie Kenny	

Target audience

All MFS	x	**Ops Crews**		**Fire safety**		**Community FS**		**Support Staff**	
Principal off.		Senior off.		etc.		etc.		etc.	

Ownership

FOI exemption required?	**Yes**		**URL**	
	No	x	Reason	

"An Excellent Authority"

Information Governance & Security Policy

Service Policy No. STRPOL09

1. Policy Introduction and Background

Information and data are necessary for Merseyside Fire and Rescue Authority (MFRA) to comply with its statutory duties and to arrange and provide services for the citizens of Merseyside.

All Members, employees, contract and temporary workers and volunteers have a responsibility to ensure that information and data are managed properly and are secure and safeguarded from inappropriate release, modification or misuse.

This includes the associated supporting technology.

Information Governance is the way in which we bring together all of the requirements and standards that apply to the handling of information on all media. This ensures that the organisation and individuals have information that is accurate, meets legal requirements, is dealt with efficiently and is secure.

2. Policy Explanation

The objective of this Information Governance, & Security Policy is to protect MFRA's information and data assets[1] from all threats, whether internal or external, deliberate or accidental, to ensure business continuity, minimise damage and maximise our ability to deliver services by bringing together all of the requirements, standards and best practice that apply to the handling of information. It has four fundamental aims:

- To support and promote the effective and appropriate use of information to deliver services;
- To encourage responsible staff to work closely together, preventing duplication of effort and enabling more efficient use of resources;
- To develop support arrangements and provide staff with appropriate tools and support to enable them to discharge their responsibilities to consistently high standards and to ensure statutory obligations are met;

[1] This includes data & information printed or written on paper, stored electronically, and transmitted by post or electronic means, stored on tape or video, spoken in conversation.

- To enable the organisation to understand its own performance against its objectives.

Information Governance and security currently encompasses:

- Data Protection Act 1998
- Freedom of Information Act 2000
- Protection of Freedoms Act 2012
- Environmental Information Regulations 2004
- Information Sharing
- The Confidentiality Code of Practice
- Records Management
- Information Quality Assurance
- Information Security
- Information Governance Management
- Risk Management
- Protective Security

Scope

The scope of this Information Governance & Security Policy covers all MFRA information and data held in any format and in any location including that held and used by Partner Organisations delivering services on behalf of the MFRA.

Policy

It is the policy of MFRA to ensure that:

- Information and data are protected from the loss of confidentiality[2], integrity[3] and availability[4].
- Legislative and regulatory requirements are met[5].
- Business continuity plans are produced, maintained and tested.
- Information security awareness training is made available to all employees and Members.
- All breaches of information and data security, actual or suspected, are reported to, and investigated by, the Information Security Forum and designated officers, and escalated to the Senior Information Risk Owner (SIRO); the Director of Strategy & Performance.
- All Strategic Management Group members and heads of department are responsible for implementing the Information Governance & Security Policy within their respective business areas.
- It is the responsibility of each member, employee, contract and temporary workers and volunteers to adhere to this policy.

3. Policy Implementation

This Policy relates to the following Service Instructions and Policy.

SI 0437 Freedom of Information requests and Publication Scheme
SI xxxx CCTV Use
SI 0759 Destruction of Information Assets (including protectively marked document)

[2] Confidentiality: ensuring that information is accessible only to authorised individuals.
[3] Integrity: safeguarding the accuracy and completeness of information and processing methods.
[4] Availability: ensuring that authorised users have access to relevant information when required.
[5] Includes legislation such as the Data Protection Act 1998, Freedom of Information Act 2000 and the Computer Misuse Act 1990.

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