



**Service Policy: STRATPOL09
Information Governance and
Security Policy**

This is an unpublished work, the Copyright in which vests in Merseyside Fire & Rescue Service. All rights reserved. The information contained herein is the property of Merseyside Fire & Rescue Service, and is supplied without liability for errors or omissions. No part may be reproduced or used except as authorised by Contract or other written permission. The Copyright and the foregoing restriction on reproduction and use extend to all media in which information may be embodied ©

Document Control:

Active date	Review date	Author	Editor	Publisher
MAY 2018	April 2027			

Amendment History:

Version	Date	Author	Reasons for Change
1	October 2013		Combined Information Governance, Data Protection & Security Policy.
1.1	November 2014		Extra Information inserted to note SI 0725 and 0433
1.2	July		Extra Si numbers added
1.3	September 2016		Review and update
1.4	April 2017		Review and update
1.5	October 2017		Updated to reflect actions taken for GDPR.
1.6	March 2018		Annual Review and update for GDPR
1.7	March 2019		Annual review
1.8	March 2020		Annual Review – details of new Data Protection Officer
1.9	April 2021		Annual Review
1.10	April 2023		Annual Review
1.11	April 2024		Annual Review and minor admin. changes
1.12	October 2024		Minor paragraph addition to make clear our ethical approach.
1.13	March 2025		Annual Review, including correction of incorrect SI titles.
1.14	March 2026		Annual Review

Equalities Impact Assessment:

Initial	Full	Date	Reviewed by	Comments
	X		ED&I TEAM	LOCATED ON PORTAL

Civil Contingencies Impact Assessment:

Date	Reviewed by	Comments

Related Documents:

Doc. Type	Ref No.	Title	Location
Service Instruction	SI 0435	Protection of Personal Data and Sensitive Business Information	1.5
Service Instruction	SI 0437	Freedom of Information Requests, Environmental Information Regulations and the Publication Scheme	1.3
Service Instruction	SI 0725	Closed Circuit Television (CCTV) Use Operated by MFRA	1.3
Service Instruction	SI 0759	Destruction of Information Assets Including Protectively Marked Information	2.3
Service Instruction	SI 0687	Preparing and Transferring Records to the RM Archive Store – Vesty Building	3.2
Policy	ICTPOL03	Acceptable Use Policy	
Service Instruction	SI0703	Internet Access and Usage	

Service Instruction	SI0730	Email	
Service Instruction	SI0699	Using Social Media	
Service Instruction	SI 0433	Retention of Information	
Service Instruction	SI 0816	Protective Marking – Government Security Classifications and Government Protective Marking Scheme	
Service Instruction	SI 0818	Security Vetting	
Service Instruction	SI 0829	Processing Vulnerable Person Data and Information (Tier 3 Protocol)	

Distribution List:

Name	Position	Department
ALL MFRS		

Sign-Off List:

Name	Position

Target Audience:

All MFRS	<input checked="" type="checkbox"/>	Ops Crews	<input type="checkbox"/>	Fire Protection	<input type="checkbox"/>	Fire Prevention	<input type="checkbox"/>
Principal officers	<input type="checkbox"/>	Senior officers	<input type="checkbox"/>	Non uniformed	<input type="checkbox"/>		<input type="checkbox"/>

Ownership:

FOI exemption required?	Yes	<input type="checkbox"/>	URL	
	No	<input checked="" type="checkbox"/>	Reason	

Legislation:

Title	Protection of Freedoms Act 2012
	UK General Data Protection Regulation 2018
	Freedom of Information Act 2000
	Data Protection Act 2018
	Human Rights Act 1998

Contact:

Department	Email	Telephone ext.
STRATEGY & PERFORMANCE		

STRATPOL09 Information Governance and Security Policy

1. Policy Introduction and Background:

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

visitors to the area.

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.

MFRA has a well-developed *ethical approach* to managing data. Ethics is not just a component of a policy for us; it is ingrained throughout our culture. We prioritise *integrity, inclusiveness, reliability, transparency* and *accountability*, and ensure that all employees are prepared to handle data responsibly and with *fairness*. We treat all data subjects with dignity; safeguarding their rights, preferences, *privacy and security*. By embedding these principles into our operations, we strive to foster trust and confidence among our data subjects, and constantly reinforce our dedication to ethical data management as a cornerstone of our organisation.

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. It satisfies the information security principles of Confidentiality, Integrity and Availability.

The Authority will process personal data in line with the requirements of the UK General Data Protection Regulation (UKGDPR) 2018 and Data Protection Act (DPA) 2018 and will take all steps necessary to ensure compliance with the legislation. The UKGDPR and DPA require public bodies to appoint a Data Protection Officer (DPO) and this role is performed for Merseyside Fire and Rescue Authority by the Director of Strategy and Performance.

2. Policy Explanation:

The objective of this Information Governance and Security Policy is to protect MFRA's information and data assets¹ from all threats, whether internal or external, deliberate or accidental, to ensure business continuity, minimise damage and maximise the Authority's 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;
- To enable the organisation to understand its own performance against its objectives.

Information Governance and Security includes compliance with:

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.

- The UKGDPR 2018
- The DPA 2018
- UK Data (Use and Access) Act 2025
- Freedom of Information Act (FOIA) 2000
- Protection of Freedoms Act (POFA) 2012
- Environmental Information Regulations (EIR) 2004
- Computer Misuse Act 1990
- Human Right Act 1998

It encompasses:

- 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 and Security Policy covers all MFRA information and data held in any format and in any location including that held and used by Partner Organisations or contractors 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 confidentiality², integrity³ and availability⁴.
- Legislative and regulatory requirements are met⁵.
- 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 as soon as possible to the DPO and subsequently investigated. The DPO is required to report such breaches to the Information Commissioner's Office (ICO) within 72 hours of becoming aware

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 General Data Protection Regulation 2016, Freedom of Information Act 2000 and the Computer Misuse Act 1990.

of a breach.

- All Strategic Leadership Team (SLT) members and heads of department are responsible for implementing the Information Governance and Security Policy within their respective business areas.
- It is the responsibility of each member, employee, contract & temporary worker and volunteer to adhere to this policy and associated Service Instructions.

3. Policy Implementation:

This Policy relates to the following Service Instructions and Policy.

SI 0435	Protection of Personal Data and Sensitive Business Information
SI 0437	Freedom of Information Requests, Environmental Information Regulations and the Publication Scheme
SI 0725	Closed Circuit Television (CCTV) use Operated by MFRA
SI 0759	Destruction of Information Assets Including Protectively Marked Information
SI 0687	Preparing and Transferring Records to the RM Archive Store – Vesty Building
SI 0829	Processing Vulnerable Person Data and Information (Tier 3 Protocol)
SI 0433	Retention of Information
ICTPOL03	Acceptable Use Policy
SI 0703	Internet Access and Usage
SI 0699	Using Social Media
SI 0730	Email
SI 0816	Protective Marking – Government Security Classifications and Government Protective Marking Scheme
SI 0818	Security Vetting

All Policies can be found on the [Website](#)