MERSEYSIDE FIRE AND RESCUE AUTHORITY			
MEETING OF THE:	**AUTHORITY**		
DATE:	**12 APRIL 2018**	**REPORT NO:**	**CFO/022/18**
PRESENTING OFFICER	**CHIEF FIRE OFFICER**		
RESPONSIBLE OFFICER:	**DEB APPLETON**	**REPORT AUTHOR:**	**DEB APPLETON JANET HENSHAW**
OFFICERS CONSULTED:	**STRATEGIC MANAGEMENT GROUP**		
TITLE OF REPORT:	**GDPR UPDATE AND INFORMATION GOVERNANCE SECURITY POLICY**		

APPENDICES:	**APPENDIX A:** INFORMATION GOVERNANCE AND SECURITY POLICY

Purpose of Report

1. To inform Members of the implications of the introduction of the General Data Protection Regulation on 25th May 2018 and request that Members consider and approve the Authority's Information Governance and Security Policy (Appendix A), which has been revised to reflect this legislative change.

Recommendation

2. That Members;

   a. Note the implications of the introduction of the General Data Protection Regulation and the actions being taken to prepare for implementation.
   b. Approve the revised Information Governance and Security Policy.

Introduction and Background

General Data Protection regulation overview

3. On 25th May 2018 the General Data Protection Regulation (GDPR) will replace the Data Protection Act 1998 and will have an impact on the way in which MFRA processes personal data. The GDPR applies to processing carried out by organisations operating within the EU. It also applies to organisations outside the EU that offer goods or services to individuals in the EU and therefore will apply to the UK even after Brexit. The UK Government is also currently in the process of introducing a new Data Protection Act which is currently progressing through the parliamentary process.

4. The GDPR provides one set of rules for processing personal data across the European Union and this is intended to make it simpler for services and business.

5. The GDPR applies to 'controllers' **and** 'processors'. The definitions are broadly the same as under the current Data Protection Act – i.e. the controller says how and why personal data is processed and the processor acts on the controller's behalf. MFRA is the data controller for all the personal information it collects directly from individuals, but is also a data processor in relation to personal data that is shared with it by other organisations. Similarly, other organisations (such as software providers or partner organisations) act as data processors in relation to information for which MFRA is the data controller.

6. The GDPR places specific legal obligations on processors; for example, to maintain records of personal data and processing activities and there is significantly more legal liability if a processor is responsible for a breach of the GDPR. These obligations for processors are a new requirement under the GDPR. The Regulator (the Information Commissioner) will have authority to issue penalties equal to the greater of 10 million euros or 2% of the organisation's gross revenue for breaches of record keeping, notification of breaches and privacy impact assessment breaches.

7. However, controllers are not relieved of their obligations where a processor is involved. The GDPR places further obligations on controllers to ensure their contracts with processors comply with the GDPR, only using those processors that provide " sufficient guarantees to implement appropriate technical and organizational measures" to meet GDPR requirements and protect date subjects' rights.

8. The major differences between the Data Protection Act 1998 and the GDPR are outlined below.

<u>Key differences between the Data Protection Act 1998 and the General Data Protection Regulation</u>

DPA(Data Protection Act) 1998	GDPR (General Data Protection Regulation)
The Data Protection Act was developed to give protection and lay down rules about how data about people can be used. The 1998 Act covers information or data stored on a computer or an organised paper filing system about living people.	EU General Data Protection Regulation (GDPR) in Europe, adopted in 2016, will be directly applicable starting on May 25, 2018, and will replace the DPA
Only applies the UK	Applies to the whole of the EU and also to any global company which holds data on EU citizens

Enforced by the Information Commissioner's Office (ICO)	Compliance will be monitored by a Supervisory Authority (SA) in each European country. In the UK this will be the Information Commissioner.
Under the current legislation there is no need for any business to have a dedicated Data Protection Officer (DPO)	A DPO will be mandatory for public sector organisations or any business or organisations with more than 250 employees. For MFRA the DPO will be the Monitoring Officer and Solicitor to the Authority.
There is no requirement for an organisation to remove all data they hold on an individual	An individual will have the right to request erasure of any data (including web records) with all information being permanently deleted (unless there is a legal reason for it to be retained)
Privacy Impact Assessment (PIA) are not a legal requirement under DPA but has always been 'championed' by the ICO	PIAs will be mandatory and must be carried out when there is a high risk to the freedoms of the individual. A PIA helps an organisation to ensure they meet an individual's expectation of privacy
Data collection does not necessarily require an opt-in under the current Data Protection Act	The need for consent underpins GDPR. Individuals must opt-in whenever required and there must be clear privacy notices. Those notices must be concise and transparent and consent must be able to be withdrawn at any time
Direction sets aims and requirements, implemented through national legislation	Regulation is binding for all member states
Personal data and sensitive personal data	In addition to existing categories of sensitive data, this now includes online identifiers, location data, and genetic/biometric data.
Breach notifications not mandatory for most organisations	Notification of a breach of the GDPR is mandatory and must be made within 72 hours to the Information Commissioner’s Office.
Any person who has material damage as a result of a breach is entitled to claim compensation	Any person who has suffered material or non-material damage a as result of a breach is entitled to claim compensation.

Data protection governance is down to best endeavours	MFRA (as with other public sector organisations) must appoint a Data Protection Officer.
Maximum fine for a breach of the Data Protection Act is £500,000	Maximum fine 4% of annual turnover or Euro20M whichever is greater
Responsibility for compliance with the Act rests with the Data Controller	Responsibility rests with both the controller and processor with the controller being able to seek damages from the processor
Parental consent for minors not required	Parental consent for minors (under the age of 13) now required
Accountability is limited to controllers	Accountability fully explicit and applies to both processors and controllers
Subject access requests, £10 per transaction and information provided to the Data Subject within 40 days	Free of charge and information must be provided within 30 days
Data consent free given, specific and informed	Clear affirmation action not just freely given, specific and informed but also unambiguous, demonstrable and explicit for Special Categories of data) with the ability to be withdrawn later. Further, there should be no silence or opt out

Action taken to implement the GDPR

9. A project group that includes the Data Protection Officer, Senior Information Risk Owner (the Director of Strategy and Performance) and information governance, ICT, People and Organisational Development and Legal staff has been working for several months to prepare MFRA for the transition from the Data Protection act to the GDPR.

10. This group is carrying out a number of activities including the following:

- Reviewing policies, procedures and Service Instructions
- Compiling an information asset register – including reviewing the reasons why information is collected
- Carrying out Privacy Impact Assessments
- Preparing Privacy Notices
- Providing advice and information about the changes to staff
- Working with suppliers (data processors) to ensure they are prepared for GDPR.

11. The attached Information Governance and Security Policy is the Authority's foundation for this work and a revised version that reflects the requirements of GDPR is attached at Appendix A for Members consideration.

Equality and Diversity Implications

12. There are no equality and diversity implications arising from this report.

Staff Implications

13. The Data Protection Officer has carried out briefings with departmental teams and internal communications have been disseminated and are planned for the future to ensure that staff are aware of their obligations. A number of staff from all departments are involved with the review and updating of policies and procedures.

Legal Implications

14. The GDPR is an important piece of legislation that will have implications for many organisations across the EU. The Data Protection Bill which is currently in the House of Lords Committee stage will mirror much of the GDPR but will also provide some additional special categories of sensitive data and make other "derogations" from the GDPR.

Financial Implications & Value for Money

15. There are no financial implications arising from this report.

16. Because the Monitoring Officer and Solicitor to the Authority has taken on the role of Data Protection Officer this has negated the need to identify additional funds to recruit to this statutory post, which even as a part time post would have cost in the region of £16,000 per year. This arrangement will be reviewed after a year, to determine if combining the roles is the best approach.

Risk Management, Health & Safety, and Environmental Implications

17. As MFRA already has comprehensive policies and procedures in relation to Data Protection it is in a relatively good position in relation to mitigating the risks associated with the introduction of the new legislation. However, a significant amount of work has already been done and remains to be done.

Contribution to Our Mission: *Safer Stronger Communities – Safe Effective Firefighters*

18. The work currently being carried out in relation to the GDPR will ensure that the Authority is compliant with the new legislation and that the personal data of staff and citizens is protected.

BACKGROUND PAPERS

CFO/111/11 If this report follows on from another, list the previous report(s)

GLOSSARY OF TERMS

MFRA	**M**erseyside **F**ire and **R**escue **A**uthority is the physical and legal entity. When writing reports MFRA is the “object”.
MFRS	**M**erseyside **F**ire and **R**escue **S**ervice is the service provided by MFRA. When writing reports MFRS is the “action”
E.G.	You are employed by the Authority (MFRA). The job you do forms part of the Service (MFRS) provided by the Authority (MFRA). If in doubt use MFRA.