CITY OF WOLVERHAMPTON COUNCIL

Pensions Board

24 January 2017

Report title	Preparing for the General Data Protection Regulations (GDPR)	
Originating service	Pensions	
Accountable employee(s)	Rachel Howe	Head of Governance
	Tel	01902 552091
	Email	Rachel.howe@wolverhampton.gov.uk
Report to be/has been considered by	Rachel Brothwood	Director of Pensions
	Tel	01902 551715
	Email	Rachel.brothwood@wolverhampton.gov.uk

Recommendations for noting:

The Board is asked to note:

1. The proposed workplan of the Fund in preparing for the changes to Data Protection Regulation.

1.0 Purpose

1.1 To provide the Board with an outline of the project plan for preparing for the changes to the Data Protection Regulations coming into force in 2018.

2.0 Background

2.1 The General Data Protection Regulation was adopted on 27 April 2016. It comes into force after a two year transition period. Unlike previous EU Data Protection legislation it does not require formal adoption by the UK and will become law on 25 May 2018.

2.2 The Changes to Data Protection have been created due to technological advances and the availability of personal information being much more widespread. New technology brings new threats and the media is full of stories of organisations which have been the victim of complex cyber-attacks resulting in personal data about their customers or employees being stolen.

2.3 Whilst there has been a lot of focus on some of the more sophisticated attacks, the most breaches come about as a result of organisations failing to get the basics right. In this regard it is worth remembering that the Data Protection Act requires organisations to have in place both ‘technical’ (It software and physical security) and ‘organisational’ (working practices) measures to keep personal data safe. In other words compliance is as much about data protection awareness, as it is about having clever technology.

3.0 The new principles

3.1 The principles set out in the GDPR are similar to those in the Data Protection Act with added details for accountability. The GDPR now requires organisations to show how they comply with the principles by documenting decisions and publishing details about processing activity.

3.2 The new principles setting out how organisations should manage their data are

(a) processed lawfully, fairly and in a transparent manner in relation to individuals;

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

4.0 Work over the next 12 months

4.1 Last year the Fund undertook an external assessment of its Information Governance procedures achieving a satisfactory level 2 out of 3. Since then we have been working to ensure our procedures meet level 3 (exemplary criteria). The Fund has completed this work and is now reviewing those processes to identify further developments to meet the GDPR requirements.

4.2 Attached at Appendix One is the proposed workplan for the Fund over the next 12 months as it works to meet the May 2018 date for compliance.

4.3 The main areas of work will be centred on the information published by the Fund about how it uses personal data. In addition we will need to review our third party contracts ensuring they comply with the new requirements which impose a greater level of responsibility on third party data processors.

4.4 The Fund is engaging with our administration software supplier, Civica, to ensure they are able to assist the Fund to fully comply with the requirements around data retention, and data portability. In addition the Fund is working with Wolverhampton City Council's Information Governance Team to ensure our work compliments each other through shared learning and efficiencies. The Council's Director of Governance is the Senior Information Officer and holds this role for the Fund also.

5.0 Financial implications

5.1 Information Governance forms part of the Fund's work and is accounted for in the annual budget. Under the GDPR the Fund will no longer be able to charge the £10 administration fee for dealing with Data Access Subject Requests and it will have to absorb this cost.

5.2 Under the Data Protection Act, the £10 charge for subject access requests is considered a deterrent by some organisations and it is likely that requests will increase once the charge is removed. This year the Fund received 4 subject access requests, each taking roughly 10 hours of officers time to compile.

6.0 Legal implications

6.1 While the new Regulation is an EU law, despite Brexit most commentators believe it will be adopted into UK law as it will come into force before Article 50 takes full effect, it is likely to be adopted thereafter. Failure to adhere to the Regulation may result in the Fund facing significant enforcement from the Information Commissioner.

6.2 Under the GDPR the level of sanction has increased greatly, with the potential for a fine up to €20 million or 4% of worldwide turnover. Under the current Data Protection Act, sanctions are limited to a fine of £500,000 with improvement/enforcement notices being imposed on organisations.

7.0 Equalities implications

7.1 None at this time, however each new policy to be written for the Fund will be assessed under the Equalities Act.

8.0 Environmental implications

8.1 None

9.0 Human resources implications

9.1 None

10.0 Corporate landlord implications

10.1 None

11.0 Schedule of background papers

11.1 General Data Protection Regulations
http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679

12.0 Appendices

12.1 Appendix 1
GDPR Workplan 2016/2017