Bath & North East Somerset Council	
MEETING:	**LOCAL PENSION BOARD**
MEETING DATE:	**19 July 2018**
TITLE:	**PENSION FUND ADMINISTRATION** **GDPR IMPLEMENTATION UPDATE**
WARD:	**ALL**
AN OPEN PUBLIC ITEM	
List of attachments to this report: Appendix 1 – GDPR Project Plan Appendix 2 – Full Privacy Notice Appendix 3 – Memorandum of Understanding	

1 THE ISSUE

1.1 The purpose of this report is to present to the Pension Board a summary of the Fund's implementation of the General Data Protection Regulation (GDPR) 2016 which came into force on 25th May 2018.

1.2 While GDPR builds on the principles established by the 1998 Data Protection Act, there are a number of actions that Pensions Schemes are required to take to achieve compliance.

1.3 The Fund has reviewed requirements provided by the Information Commissioners Office (ICO) and worked with B&NES Council Data Protection Officer (DPO) in developing a project plan to assist in the implementation of GDPR.

2 RECOMMENDATION

The Board is asked to note the Fund's progress on the implementation of GDPR

3 BACKGROUND

3.1 Since 1948 various pieces of legislation on data protection have been introduced, most notably the Data Protection Act 1998, which set down eight overarching principals. The GDPR, effective from 25th May 2018 has brought about a sea change of in the way that data processing is regulated across the entirety of the EU.

3.2 The introduction of the GDPR has been in response to the changing ways in which personal data is managed. In particular, the use of software and the communication and controlling of transferred personal data via the internet. Personal data is now recognised as a commodity, and whilst the Fund has already protected that commodity in accordance with the Data Protection Act 1998, it is now required to ensure that the protections are appropriate for the modern age.

3.3 As at 31st March the Fund membership was estimated at 110,225. Each member record contains multiple items of personal data. The Pension Regulator (tPR) categorises this personal data in terms of common and conditional (scheme specific) data and in turn sets the Fund quality standards by which that data must be measured and maintained.

3.4 Whilst the Pensions Regulator sets the quality standards, it is the ICO that oversees the requirements of GDPR, in particular the Fund's management of personal data and its right to lawfully process it. Asa Data Controller, the Fund on behalf of Bath & North East Somerset Council is therefore required to undertake a review of its policies and procedures to ensure that all parties involved in the management of members personal data are compliant with GDPR requirements.

4 KEY STEPS TAKEN BY THE FUND TO COMPLY WITH GDPR

4.1 The Fund has completed the ICO self-assessment checklist in conjunction with the 12 step GDPR preparation guide to produce a comprehensive project plan (Appendix 1). A number of key Fund actions have been identified, in particular;

- to undertake a data mapping exercise, including flowcharts to identify data flows and the processes being applied to such data. As part of the exercise all risks identified will be RAG rated.

- to undertake DPIA to ensure that all significant changes made by the Fund which impact on the processing of personal data are validated.

- to undertake a review of the process for ill health retirements to ensure explicit consent satisfied.

- to undertake to review all 3rd party contracts to ensure GDPR compliant

- Training – all staff are required to undertake B&NES online training module. Training undertaken is monitored and recorded. Currently 95% of admin staff have undertaken the e-learning module.

5 COMMUNICATION ACTIVITY

5.1 The GDPR requires additional content to be included in all privacy notices regarding how personal data will be used by data controllers. The administration authority, as a data controller, must tell anyone whose personal data they collect what information is held, how it is used, who it may be shared with and what safeguards are in place.

5.2 A privacy notice template was produced by the LGA in conjunction with their legal advisors. APF adopted and adapted this template which was ratified by

B&NES DPO (Appendix 2). The privacy notice has been published on the Funds member website prior to 25th May.

5.3 Reference to data protection and the privacy notice is now included on all Fund administration letters, forms, factsheets and new member information packs, with a link to the full privacy notice on the website.

5.4 In addition to information on the member website, information articles on GDPR have been included in publications of newsletters for all active, deferred and pensioner members.

5.5 The *my pension online* system, where members can access their own pensions data via a secure online portal, now has a consent element, which members have to check in order to access the system. The system also retains their acknowledgement of consent.

6 MEMORANDUM OF UNDERSTANDING FOR SCHEME EMPLOYERS

6.1 The LGA produced a template for a memorandum of understanding (MOU) for Scheme Employers (Appendix 3). This document sets out expectations and standards required between the two data controller organisations.

6.2 Under GDPR there is no legal requirement to have individual signed agreements between the Fund and Scheme Employer. The fund adopted the template before communicating it to all employers (350+) in May. The MOU will be incorporated in each employer service level agreement when the Pensions Administration strategy is reviewed later this year.

7 NEXT STEPS

7.1 GDPR became effective from 25th May 2018. The Fund has commenced various activities with the aim of working towards full compliance. Progress against the Project Plan will be presented at future Pension Board and Pension Committee meetings for approval.

7.2 Once established the Fund will undertake a periodic review of GDPR arrangements to ensure continued compliance with its principals as determined by the ICO.

8 RISK ASSESSMENT

8.1 There are no direct risks to the Fund associated with this report although any failure to hold personal data securely is covered under R05 on the Risk Register.

9 EQUALITIES

9.1 No items in this report give rise to the need to have an equalities impact assessment

10 CONSULTATION

10.1 None appropriate

11 ISSUES TO CONSIDER IN REACHING THE DECISION(S)

11.1 There are no issues to consider not mentioned in this report.

12 ADVICE SOUGHT

12.1 The Council's Monitoring Officer (Divisional Director – Legal & Democratic Services) and Section 151 Officer (Strategic Director of Resources) have had the opportunity to input to this report and have cleared it for publication.

Contact person	*Geoff Cleak – Pensions Manager; Tel 01225 395277*
Background papers	*Various GDPR documentation and guidance information issued by Information Commissioners Office.*
Please contact the report author if you need to access this report in an alternative format	