CITY OF WOLVERHAMPTON COUNCIL

Pensions Committee

12 December 2018

Report title	GDPR Audit Review	
Originating service	Pension Services	
Accountable employee(s)	Rachel Howe	Head of Governance and Corporate Services
	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

Recommendation for noting:

The Committee is asked to note:

1. The Fund's compliance with the requirements of the General Data Protection Regulations and Data Protection Act 2018 as confirmed in the internal and external audit reviews commissioned by the Fund's Data Protection Officer.

1.0 Purpose

1.1 To update Committee on the work of the Fund to prepare and comply with the changes to Data Protection Law that came into effect in the UK on 25 May 2018.

1.2 To provide assurance as to the completion of that work in the review of the Fund by internal and external audit bodies.

2.0 Background

2.1 The EU General Data Protection Regulation (GDPR) came into effect on 25 May 2018 and replaced the previous version from 1995. Prior to it coming into effect, the UK Government enacted the Data Protection Act 2018 which sought to implement the EU legislation into UK law. Both pieces of legislation should be read in conjunction with one another and will be referred to jointly as “Data Protection Laws” throughout this report.

2.2 The Data Protection Laws were designed to harmonise data privacy laws and empower individuals in the management of their data by public and private sector organisations. The Data Protection Laws impose a greater duty on organisations to be open and transparent with individuals about how they use their data with greater opportunity to restrict and refuse that use being given to the individual.

2.3 In preparation for the changes, the Fund worked with a number of LGPS Funds across the Country to formalise our approach in the application of Data Protection Laws to our working practices. Working with the LGA, the Funds devised a number of template documents for circulation across the LGPS Funds, including the production of a Memorandum of Understanding which defined the Joint Data Controller relationship with our employers.

3.0 Internal Audit Review

3.1 Prior to the implementation of the Law in May 2018, Internal Audit at the City of Wolverhampton Council undertook an assessment of the Fund’s preparation for the changes in November 2017, in line with the guidance from the Information Commissioner (ICO), using their 12 steps to GDPR as a basis for assessing our preparations. At that time the Fund were deemed to be on course with our work with no significant issues highlighted.

3.2 Acknowledging that assessment was undertaken as part of our preparation, and with a number of steps still in progress at the time of the internal audit, a follow up assessment was requested in October 2018 to ensure that all steps required for compliance with the Law had been implemented.

3.3 Aside from some minor actions (where policies were still noted as draft, having been fully implemented) the internal audit review showed good compliance with the Data Protection Law noting the work the Fund had done to inform members of their rights and access to

information under GDPR. A number of areas of good practice were highlighted as noted in the report attached at Appendix A.

4.0 External Audit Review

4.1 To further strengthen the Fund's compliance with Data Protection Law, an external company were appointed to undertake a review of the Fund in line with wider national and industry organisations. The Fund had previously been assessed by an external company in 2015 and were found to be highly compliant and were keen to ensure this ongoing high standard under the new requirements.

4.2 The external audit found a number of areas of good practice and compliance with the requirements of the GDPR, with a number of areas to be updated to ensure complete compliance.

4.3 Overall the Fund scored a satisfactory rating noting it to be 82% compliant with the requirements of Data Protection Law. Areas for improvement that were noted were policies had been drafted prior to 25 May and required updating to ensure it read as current not future tense. Work continues to develop some of the Fund's monitoring practices in relation to its Information Asset Register.

4.4 The Fund's Data Protection Officer will now undertake actions to ensure the areas for improvement are fully embedded.

5.0 Financial implications

5.1 The cost of implementing GDPR is included in the Fund's Service Development Budget.

5.2 Failure to adhere to the changes could result in fines of up to €20,000,000 or 4% of turnover.

6.0 Legal implications

6.1 The Data Protection Law came into effect on 25 May 2018, the ICO has stated that provided bodies are taking steps to become compliant with the changes, they will not take action or impose severe fines within the first 12 months of it coming into force.

6.2 However, there is a significant risk to the Fund of reputational impact should the Fund not comply with the requirements of GDPR, not least the lack of confidence from our members and employers in our ability to manage and protect their personal data.

7.0 Equalities implications

7.1 The GDPR policy and the Privacy Impact Assessments have been drafted in line with the Equalities Act.

8.0 Environmental implications

8.1 There are no implications

9.0 Human resources implications

9.1 There are no implications

10.0 Corporate landlord implications

10.1 There are no implications

11.0 Schedule of background papers

11.1 ICO guide to the General Data Protection Regulations
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

11.2 Data Protection Act 2018
http://www.legislation.gov.uk/ukpga/2018/12/contents

11.3 External Audit report

12.0 Schedule of Appendices

12.1 Appendix A: Internal Audit report