Final Internal Audit Report:

GDPR Review

2018/2019

wolverhampton.gov.uk

CITY OF WOLVERHAMPTON COUNCIL

1. Executive summary

Introduction

Following the introduction of the General Data Protection Regulation (GDPR) in May 2018 an audit is proposed as part of the approved internal audit plan for 2018/19. This review aims to provide assurance that the controls and procedures implemented have been fully embedded within the Fund and are operating effectively.

Scope and objectives of audit work

Our audit will be conducted in conformance with the Public Sector Internal Audit Standards and will consider the following objectives, and the potential risks to the achievement of those objectives:

- Provide excellent customer service

The review will be based on the Information Commissioner's Office (ICO) guide to undertaking information audits which covers the key areas of information governance.

Scope	Potential risks
The audit will include a review of the following: • Governance arrangements for GDPR • Records management • Subject Access Requests • Training and awareness • Data sharing, including third party member information requests. • Information risk management • Direct marketing	• Regulatory action for failure to comply with legislative requirements • Financial penalties • Loss of sensitive information • Reputational damage through adverse reports

Limitations to the scope of our audit
A high-level review of operational controls and sample testing of areas included in the scope.

Overall conclusion

Taking account of the issues identified in this report, in our opinion the controls operating within the system, provide only **satisfactory assurance** as part of the process to mitigate risks to an acceptable level.

Limited	**Satisfactory**	Substantial
There is a risk of objectives not being met due to serious control failings.	**A framework of controls is in place, but controls need to be strengthened further.**	There is a robust framework of controls which are applied continuously.

Key issues identified

We have identified no significant issues. However, we have raised five issues classified as green which are further detailed in section two of this report.

Examples of good practice identified

During our work we identified the following examples of good practice in the management of risk, as achieved through the effective design and application of controls:

Robust information governance arrangements including:

- An updated 2018 Data Protection policy (final document to be published on the Fund's website);
- An updated governance section available to members on the Fund's website;
- Established reporting lines for information governance issues;
- Formalised roles for information governance including an appointed Data Protection and Governance Officer;
- Fund membership of the Council's Information Governance Board;
- Formalised risk registers are maintained which includes reference to GDPR.

Record management controls are in place including:

- An updated 2018 Record Management policy;
- Defined record management roles and responsibilities;
- Information asset registers recording Fund data;
- An updated privacy notice has been published on the Fund's website setting out the Funds retention policy.

Subject Access Requests:

- Established procedures for managing and monitoring SARs within mandatory timescales are in place which is included in the privacy notice published in the fund's website.

Training and awareness:

- The Fund provides new and existing staff with information governance training;
- Central training records are maintained and monitored.

Data sharing, including third party member information requests:

- Data sharing arrangements are governed as part of data sharing agreements;

Information risk management:

- Established procedures for managing, investigating, reporting and monitoring breach incidents are in place in line with Council procedures which the Fund has adopted;
- Reporting of breaches are taken to the Council's Information Governance Board, the Fund's Senior Management Team and Pensions Committee;
- Informed information governance decision making takes place through monitoring data captured on an incident log and risk register maintained;
- No data breach incidents have occurred since GDPR came into effect which required reporting to the ICO.

Security of personal data:

- The security of the Fund's IT systems are provided by the Council's ICT department or in the case of UPM by the system provider Civica as part of built in safeguards;
- Security of personal data is covered as part of training delivered to Fund staff;
- Physical security measures are in place at the fund to safeguard personal data;
- Suppliers IT Security is covered in data sharing agreements with the Fund.

Acknowledgement

A number of employees gave their time and co-operation during the course of this review. We would like to record our thanks to all of the individuals concerned.

2. Issues arising

Priority rating for issues identified:

Red	**Amber**	**Green**
Action is imperative to ensure that the objectives for the area under review are met	Action is required to avoid exposure to significant risks in achieving objectives	Action is advised to enhance risk control or operational efficiency

Action is advised to enhance risk control or operational efficiency **Green**		
No	**Issue arising**	**Agreed action including responsibility and target date**
2.1	The Data Protection policy 2018 published on the Funds website which had been updated for GDPR, is stated in the version history section of the document to be a first draft. However, it is acknowledged the policy was approved by the Pensions Committee and reported to the Pensions Board prior to being published on the WMPF public website. **Implication:** The Fund's Data Protection requirements may not be clearly demonstrated in the absence of a final published 2018 Data Protection policy.	The draft Data Protection policy 2018 has been published as a final policy on the website. **Responsibility:** Holly Slater, Governance Officer **Target date:** Implemented
2.2	The Records Management policy 2018 published on the Funds website is stated to be a draft document. However, the Head of Governance & Corporate Services confirmed that the policy was up to date and was based on Council policy. **Implication:** The Fund's record management requirements may not be clearly demonstrated in the absence of a final Records Management policy.	The Records Management policy 2018 has been published as a final document. **Responsibility:** Holly Slater, Governance Officer **Target date:** Implemented

2.3	At the time of audit, the Funds system provider Civica had not signed a data sharing agreement as the provider was disputing whether they were a data controller or data processor, with ongoing discussions taking place. However, the Head of Governance & Corporate Services had advised that as part of the tender for provision of the Funds system, an assurance statement covering data security had been provided by Civica. **Implication:** Assurances about the Fund's data are not provided by Civica as part of a data sharing agreement.	In the event of Civica not signing a data sharing agreement, legal advice will be sought on the contractual obligations of Civica in complying with GDPR legislative requirements. **Responsibility:** Rachel Howe, Head of Governance & Corporate Services **Target date:** As soon as possible
2.4	GDPR training was found to be included in the staff induction together with GDPR training provided to Fund staff in readiness for the implementation of GDPR. At the time of audit, arrangements for future refresher training were being considered including making completion of the Council's GDPR e learning course mandatory, which approximately one third of Fund employees had completed. **Implication:** A risk of staff not undertaking refresher training resulting in potential breaches.	Mandatory GDPR and refresher GDPR training will be undertaken annually. **Responsibility:** Holly Slater, Governance Officer **Target date:** 31 May 2019
2.5	A review of the application to join the pension scheme form on the Funds website identified that the Data Protection Statement requires updating relating to the Data Protection Act reference, e mail address for data access requests and data sharing arrangements under the National Fraud Initiative. **Implication:** The Funds Data Protection statement to members joining the Fund does not accurately report the Funds position.	The application to join the pension scheme form published on the Funds website will be updated. **Responsibility:** Holly Slater, Governance Officer **Target date:** Implemented

Limitations inherent to the internal auditor's work

This report has been prepared solely for West Midlands Pension Fund in accordance with the terms and conditions set out in the terms of reference. Internal audit does not accept or assume any liability of duty of care for any other purpose or to any other party. This report should not be disclosed to any third party, quoted or referred to without prior consent. Internal audit has undertaken this review subject to the limitations outlined below.

Internal control

- Internal control systems, no matter how well designed and operated, are affected by inherent limitations. These include the possibility of poor judgement in decision making, human error, control processes being deliberately circumvented by employees and others, management overriding controls and the occurrence of unforeseeable circumstances.

Responsibilities of management and auditors

- It is management's responsibility to develop and maintain sound systems of risk management, internal control and governance for the prevention and detection of irregularities and fraud. Internal audit work should not be seen as a substitute for management's responsibilities for the design and operation of these systems.
- Internal audit endeavours to plan audit work so that it has a reasonable expectation of detecting significant control weakness and if detected, will carry out additional work directed towards identification of consequent fraud or other irregularities. However, internal audit procedures alone, even when carried out with due professional care, do not guarantee that fraud will be detected.
- Accordingly, these examinations by internal auditors should not be relied upon solely to disclose fraud or other irregularities which may exist.

Report distribution:	Rachel Brothwood, Director of Pensions Rachel Howe, Head of Governance & Corporate Services Holly Slater, Governance Officer
Date:	22 October 2018