Agenda Item No: **13**

Pensions Committee
18 March 2015

Report title	Information Governance
Originating service	Pension Services
Accountable employee(s)	Emma Bland — Compliance and Risk Manager Tel — 01902 554387 Email — Emma.bland@wolverhampton.gov.uk
Consultees	Adam Hadley — Scrutiny and Transparency Manager Martin Eades — Information Governance and Security Officer
The Report has been considered by	Geik Drever — Strategic Director of Pensions Tel — 01902 552020 Email — Geik.drever@wolverhampton.gov.uk

---

Recommendation(s) for action or decision:

The Committee is recommended to:

1. Approve the registration of the Fund as Data Controller, with the Information Commissioner's Office (ICO).

2. Approve the terms of reference for the Information Governance Working Party and associated definitions, roles and responsibilities, as well as the proposed appointments to those roles.

3. Approve the Information Governance Policy.

4. Delegate authority to the Strategic Director of Pensions to implement the required changes.

1.0   Purpose

1.1   To seek the approval of the Committee to register the Fund as Data Controller with the ICO.

1.2   To present to the Committee the terms of reference for the Information Governance Working Party and associated definitions, roles and responsibilities, as well as recommending appointments to roles.

1.3   To present to the Committee the proposed Information Governance Policy.

2.0   Background

2.1   At the 10th December 2014 Pensions Committee, a paper was presented asking the Committee to note that under the provisions of the Data Protection Act (DPA), the Fund should register with the ICO, as being responsible for its own handling of data, i.e. a Data Controller.

2.2   The DPA states that the Data Controller is a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be processed.

2.3   The Fund falls into this category: it holds information for all members of the pension scheme and currently, holds in excess of 270,000 accounts. Whilst some of that information is also held by Wolverhampton City Council as an employer, the Fund holds other information which is not accessible by the City Council and which is not required for their purposes (as they are not the sole employer of all members of the Fund). For this reason the Fund are considered to be in control of this information, information which is sensitive personal data.

3.0   Work undertaken

3.1   Discussions were held with the City Council's Scrutiny and Transparency Manager and taking on-board the Council's experience and benchmarking of other board's across the country, it was identified that, in order to carry out its role as Data Controller and meet its obligations, the Fund should have in place:-

- **An Information Governance Policy**
  An Information Governance Policy provides guidance on information governance. It sets out objectives, scope, regulatory requirements and responsibilities. It also provides a Framework to ensure the Fund meets its obligations for the effective management of information, covering areas such as freedom of information, data protection, records management, information security and quality.

- **An Information Governance Working Party**
  The Information Governance Working Party provides high level oversight and support to the Senior Information Risk Owner (SIRO) and Data Controller. It determines the

long term information governance strategy, monitors progress against strategy and provides assurance that information risk is being properly assessed, controlled and mitigated.

- **An Information Governance Operational Group**
  The Information Governance Operational Group consists of subject matter experts and provides operational support to the organisation and the Information Governance Working Party and is responsible for ensuring that any tasks commissioned by the Working Party are effectively implemented.

3.2   The governance structure is shown in Appendix 1.

4.0   Terms of Reference, Roles, Responsibilities and Appointments

4.1   Appendix 2 sets out the terms of reference for the Information Governance Working Party and Appendix 3 sets out the related definitions, roles and responsibilities.

5.0   Information Governance Policy

5.1   The Information Governance Policy, outlined in 3.1, is attached in Appendix 4.

6.0   Next Steps

6.1   To improve Data Protection and Freedom of Information awareness, Fund Senior Managers and Team Leaders have already received training tailored specifically to the Fund.

6.2   In addition this training was cascaded to all staff at a Staff Briefing in February 2015 and will be included in Trustee induction training in July 2015.

6.3   Should the Committee agree with the recommendations, Officers will:-

- register the Fund as Data Controller with the ICO;

- set up the Information Governance Working Party and Operational Group;

- implement the Information Governance Policy and related policies and procedures.

7.0   Financial implications

7.1   There is a fee cost to the registration of the Fund as a Data Controller of £35.

7.2   In addition there is a resource implication to the Fund in setting up and adopting these policies and processes which will need to be absorbed by Fund staff as part of their current duties.

7.3   Failure to comply with the requirements could amount to a significant financial penalty from the ICO which will need to be borne by the Fund.

8.0   Legal implications

8.1   Registration by Data Controllers is a legal requirement and our failure to meet this requirement would mean we are falling foul of the legislation which would leave us open to challenge.

9.0   Equalities implications

9.1   There are no equalities implications.

10.0   Environmental implications

10.1   There are no environmental implications.

11.0   Human resources implications

11.1   Within information governance there are key roles which have to be fulfilled. These roles are identified within Appendix 2 along with the recommended posts which should fulfil them. These are:

Role	Responsible Post
Data Controller	Strategic Director of Pensions
Senior Information Risk Owner (SIRO)	Head of Governance
Caldicott Guardian (Adults)	Service Director, Older People
Qualified Person	Head of Governance
Public Interest Test	Head of Governance

11.2   Where a post is vacant or the incumbent is unable to act, the person undertaking that role shall be responsible.

12.0   Corporate landlord implications

12.1   There are no corporate landlord implications.

13.0   Schedule of background papers

13.1   Data Protection Act 1998
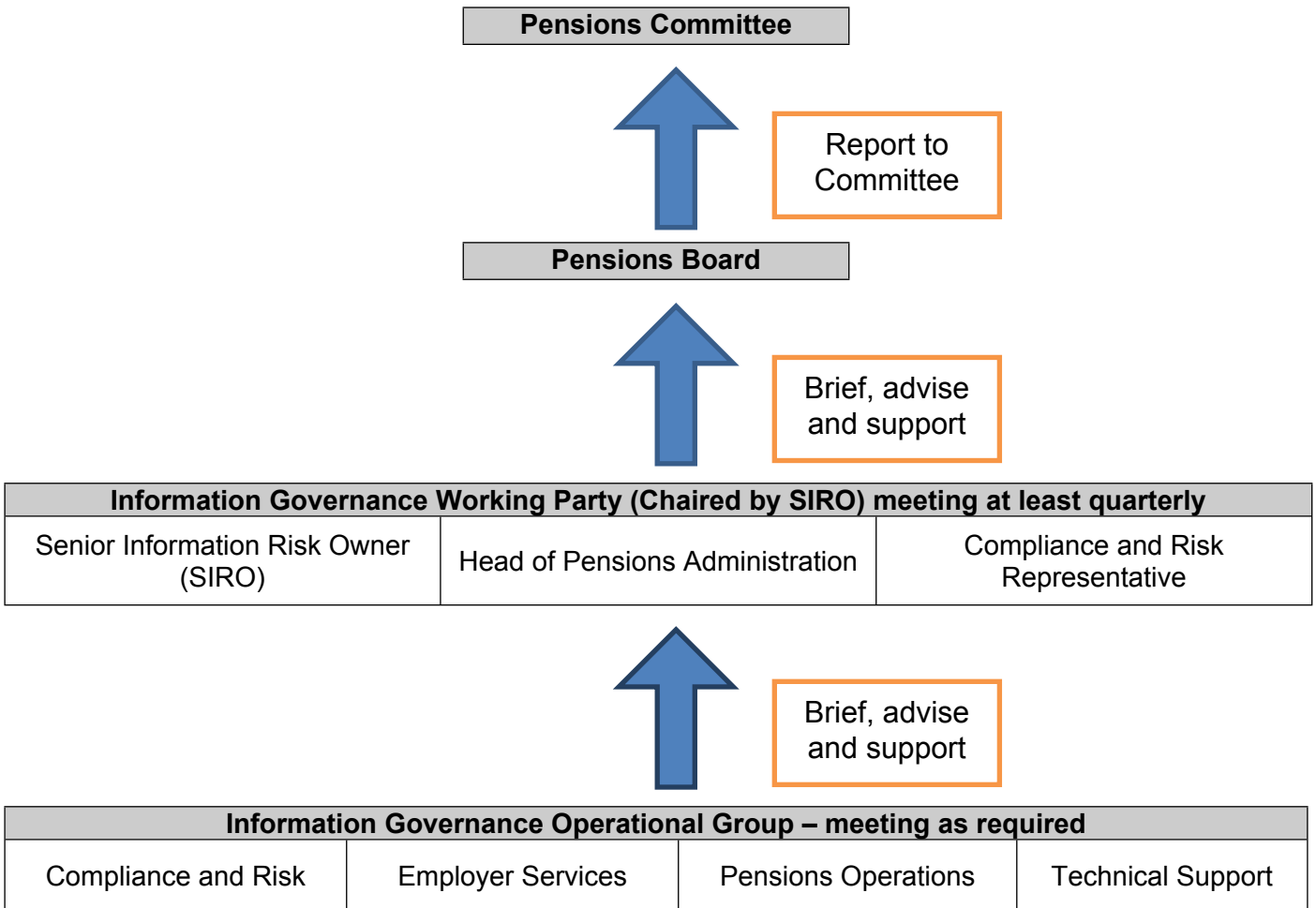http://www.legislation.gov.uk/ukpga/1998/29/contents

13.2   Pensions Committee 10 December 2014 Information Governance report
https://wolverhamptonintranet.moderngov.co.uk/documents/g4114/Public%20reports%20pack%2010th-Dec-2014%2013.30%20Pensions%20Committee.pdf?T=10

14.0   Schedule of Appendices

14.1   Appendix 1
         Information Governance Structure Chart

14.2   Appendix 2
         Information Governance Working Party - Terms of Reference

14.3   Appendix 3
         Information Governance Board – Definitions, Roles and Responsibilities

14.4   Appendix 4
         Information Governance Policy

Appendix 1

Pensions Committee

↑ Report to Committee

Pensions Board

↑ Brief, advise and support

Information Governance Working Party (Chaired by SIRO) meeting at least quarterly		
Senior Information Risk Owner (SIRO)	Head of Pensions Administration	Compliance and Risk Representative

↑ Brief, advise and support

Information Governance Operational Group – meeting as required			
Compliance and Risk	Employer Services	Pensions Operations	Technical Support

Appendix 2

Information Governance Working Party

Terms of Reference

1.   Purpose

1.1   The purpose of this Working Party is to support and drive the development of effective corporate strategies to ensure the Fund puts in place appropriate information risk management activities and complies with best practice mechanisms, legislative requirements and standards in respect of the confidentiality, integrity, availability and security of information.

2.   Objectives of the Working Party

The Working Party will:

2.1   Provide leadership, strategic direction and promote consistent standards for information governance across the Fund, to enable risk, ethical, legal, operational and policy issues to be assessed and appropriately managed;

2.2   Act as an escalation point in relation to issues raised by the Information Governance Operational Group;

2.3   Discuss, assess and provide advice and guidance to establish the amount and type of risk it is prepared to accept or tolerate in the form of an information risk appetite;

2.4   Have oversight of the information risk register, associated risk management action plan and information asset register to ensure all relevant risks are assessed and appropriate control measures and mitigation is put in place against the backdrop of agreed information risk appetites;

2.5   Ensure compliance with the Information Governance Framework, including setting levels of progress against the Information Governance Maturity Model and monitoring activities designed to achieve these set levels;

2.6   Oversee the information governance work programme;

2.7   Receive and review information governance performance statistics, seeking assurances that robust arrangements are in place to clearly communicate and incorporate any lessons learnt into corporate policies, procedures and guidelines;

2.8   Report to, and advise, Pensions Committee and councillors on any matters related to information governance that should be brought to their attention and commission the delivery of any tasks as directed by these key stakeholders;

2.9   Have an oversight of the work undertaken with outside bodies and partner

organisations, seeking assurances that barriers to information sharing are identified and overcome, innovative collaborative working practices are being developed and that information is being shared effectively, ethically and legally for the mutual benefit of all concerned;

2.10   Receive and review information governance incident reports that detail outcomes and trends, seeking assurance that common areas for improvement are incorporated into corporate policies, procedures and guidance to ensure information is suitably protected;

2.11   Own the privacy impact assessment process;

2.12   To oversee and agree to the development of new information governance policies and procedures and to support their implementation and to review and monitor existing information governance policies to maintain currency with changes in legislation;

2.13   To agree and own a necessary training programme for staff on information governance and ensure its availability to staff.

2.14   To be a member of the current 3-tier Wolverhampton Information Sharing framework.

3   Accountability

3.1   The Working Party reports to Pensions Committee and Councillors (this will predominantly be through the Pension Board).

3.2   The SIRO reports to the Strategic Director of Pensions in the form of an annual report.

4   Working Party Membership

4.1   The Working Party will be chaired by the SIRO and consist of the:

- Head of Pensions Administration;

- Compliance and Risk Team representative

Please refer to the proposed information governance structure chart in Appendix 1 and supporting Information Governance Working Party roles and responsibilities guidance document (Appendix 3).

5   Meetings and Reporting

5.1   The Working Party will meet at least quarterly. Minutes of each meeting will be produced and circulated within two weeks of the meeting.

6   Approval and Review

6.1   These terms of reference will be reviewed annually and any changes agreed
        with the SIRO and the Working Party.

Appendix 3

Information Governance Working Party

Definitions, roles and responsibilities

1. Information Governance Working Party

The Working Party provides high level oversight and support to the SIRO and Data Controller. It determines the long term information governance strategy, monitors progress against strategy and provides assurance that information risk is being properly assessed, controlled and mitigated as detailed in Appendix 2, section 2, Objectives of the Working Party.

The Working Party will be chaired by the SIRO and consist of the Head of Pensions Administration and a Compliance and Risk Team representative; all of whom will be permanent members of staff and suitably trained.

The Working Party will be supported by the Information Governance Operational Group.

2. SIRO

The SIRO will chair the Information Governance Working Party and will be supported by the Fund's Compliance and Risk Team; more specifically they will:

- Take overall ownership of the Fund's Information Governance Framework acting as champion for information governance;

- Provide advice and reports to the Strategic Director of Pensions in respect of information incidents and risks, including the content of the Fund's Annual Governance Statement in regard to information risk;

- Provide an annual report to the Strategic Director of Pensions on their work;

- Understand how the strategic goals of the Fund may be impacted by information governance risks, and how these risks may be managed including the adequacy of levels of independent scrutiny;

- Provide a focus for the management of information governance at Working Party level; and

- Owns the management of information governance and risk assessment processes within the Fund including the provision of advice on the effectiveness of information risk management across the Fund.

It is recommended that the Head of Governance is appointed to this role.

3.   **Compliance and Risk Team**

The Compliance and Risk Team will be required to adopt a strategic role for information governance and will be the champion for information governance. The Compliance and Risk Team will report on information governance matters to the Working Party and promote and develop a culture that values, protects and uses information to deliver improved services; more specifically:

- Compliance with the Fund's Information Governance Framework – promote and ensure awareness of applicable information governance policies and working practices and procedures for the effective use and protection of information assets;

- Information Management – be an advocate for and provide a focus for the management of information;

- Information Asset Information – support and promote the completion and maintenance of the Fund's Information Asset Register. This will include providing oversight of the identification of information risks as part of this process;

- Information Risk – support and promote the information risk assessment process providing assurance on security and use of information. This includes oversight of assessment, protection, response and recovery actions;

- Information Incidents – provide support and assistance to ensure compliance with the Fund's Information Incident Policy and the implementation of agreed actions in response to incidents affecting information assets;

- Information Governance Culture – foster an effective information governance culture for employees and other relevant parties who access and use the Fund's information assets to ensure individual responsibilities are understood, and that good working practices are adopted in accordance with the Fund's information governance policies. A culture that values, protects and uses information to deliver improved services.

4.   **Information Governance Operational Group**

The Information Governance Operational Group should consist of subject matter experts and provides operational support to the organisation and the Working Party and is responsible for ensuring that any tasks commissioned by the Working Party are effectively implemented.

The Group will be chaired by a Compliance and Risk Team representative and be composed of employees from the following service areas:

- Employer Services

- Pensions Operations

- Systems/Technical Team

The Group will meet as often as is required and will provide an assurance that information assets are being properly identified, recorded, risk assessed and managed in accordance with corporate policies and procedures. The Group will also be responsible for ensuring that work commissioned by the Information Governance Working Party is implemented effectively and be a collaborative platform to help develop the information governance culture.

5.   **Chair of Information Governance Operational Group**

The Chair of the Information Governance Operational Group is the lead support officer of the Working Party providing the primary link between the Operational Group and the Working Party; therefore it is recommended that a Compliance and Risk Team representative undertakes this role.

6.   **Caldicott Guardians**

The Caldicott Guardians work as part of a broader information governance function within the Council and to act as a conscience in matters of information confidentiality and sharing for social care and health information; more specifically:

- To act as champions for data confidentiality at Directorate Management level and as part of the Council's Information Governance Board;

- To provide confidentiality and data protection expertise and to develop a knowledge of confidentiality and data protection matters including links with external sources of advice and guidance;

- To ensure that confidentiality issues are appropriately reflected in Council strategies, policies and working procedures for employees;

- To oversee all arrangements, protocols, procedures and adherence to the Caldicott Principles where confidential social care information may be shared with external bodies including disclosures to other public sector agencies and other outside interests.

The Caldicott Guardian for Adults is the Service Director for Older People.

Information Governance Policy

Contents

1 Introduction

Information is a vital asset, both for the provision of services and for the efficient management of services and resources. Without it, informed, substantiated decisions cannot be made. It is of paramount importance that information is efficiently managed and that appropriate standards, policies and procedures provide a robust governance framework for information management.

2 Purpose

The purpose of this document is to outline an information governance framework that ensures West Midlands Pension Fund:-

- Meets its legal obligations for the effective management of information;
- Recognises the key enabling role of information in supporting the achievement of Fund objectives;

- Ensures that information is treated as a valuable asset.

3 Objectives

West Midlands Pension Fund will define an Information Governance Management Strategy. This will set out the strategy for the implementation of the Information Governance Framework outlined in this policy to ensure that the Fund:-

- Holds information securely and confidentially
- Obtains information fairly and efficiently
- Records information accurately and reliably
- Uses information effectively and ethically
- Shares information appropriately and lawfully

The Framework will also seek to ensure that information is available to support service improvement, transparency and openness, accountability, and open data initiatives.

4 Scope

The scope of this policy will apply to:-

- All information held and used by West Midlands Pension Fund
- All information systems operated or managed by West Midlands Pension Fund
- Any individual using information held by West Midlands Pension Fund
- Any individual requiring access to information held by West Midlands Pension Fund

This policy should be read in conjunction with the:-

- Data Protection Policy;
- Records Management Policy;
- Information Security Policy;
- Freedom of Information Policy.

5   Legal, Regulatory and Standards

There are a number of legal obligations placed upon the Fund for the use and security of information held by the organisation as well as a number of standards and best practice guides. The term Information Governance encompasses the following areas:

- Data Protection Act 1998, Privacy and Confidentiality Law and Information Sharing Best Practice
- Freedom of Information Act 2000
- Records Management Best Practice and Standards and Copyright Law
- Information Security and Information Risk Standards
- Information Quality Assurance Best Practice

6   Responsibilities

The Information Governance Working Party is responsible for the implementation of this policy and the information governance framework outlined within it. Specific responsibilities are allocated in the core information governance policies.

7   The Information Governance Framework

The framework includes the Information Governance areas already referred to above, i.e.: -

- Freedom of Information and Openness
- Data Protection and Confidentiality
- Records Management (including copyright law)
- Information Security and Risk Management
- Information Quality

For each area the following processes are required to be in place to complete the information governance framework.

7.1 Management Arrangements

For each information governance area within the framework there will be a top level policy setting out the Fund's rules, requirements and responsibilities in order to meet legislative and best practice standards. These policies will be supported by more specific policies and procedures where these are required.

The Information Governance Working Party will be responsible for the Information Governance Strategy, agreeing policies, agreeing implementation methods and improvement plans. It will also be responsible for ensuring that the processes listed below are put in place.

7.2 Training and Awareness

Each information governance area will have a planned approach to training and awareness for all policies and procedures that are agreed and implemented within the

framework. These should be role based, regularly assessed and equip each trainee with the knowledge and skills to fulfil their responsibilities.

7.3 Documented Procedures

There will be documented procedures to support agreed policies. These will specify any operational instructions required to ensure compliance with legislation and standards.

7.4 New and Changed Systems

There will be mechanisms to ensure that information governance issues are considered for all new and changed information system or deployment of ICT. The issues arising will be documented and assessed using information risk management methods where information assurance is identified as an issue.

7.5 Process Implementation - Monitoring and Compliance

There will be a timely and effective monitoring, reporting and compliance regime to support the assessment of process effectiveness.

8. Review

This policy will be reviewed annually or when required by any changes in legislation, regulations or business practice.