Information Asset Management Policy

1.0 Purpose

1.1 The purpose of this policy is to outline the management of the Fund's information asset register and the actions that will be taken to provide sufficient maintenance of the Information Asset Register for West Midlands Pension Fund. The Fund has undertaken the task of producing an information asset register in line with the Information Governance Toolkit and audit that was completed in December 2015.

1.2 The policy details the requirements and responsibilities of officers for updating and ensuring accurate representation of the Fund's information assets in the register at any point in time. This will form part of an annual update to the City of Wolverhampton Council's Information Governance Team as they are our data controller under the Information Commissioner and will give assurance that the Fund is fully compliant with information governance best practice and can provide documented information regarding the data we hold.

2.0 Scope

2.1 The Information Asset Register and supporting action plan covers all areas of the Fund, it's staff and the use of information assets outside of the normal place of work.

2.2 The Fund is required to comply with the Data Protection Act 1998 and the implementation to the change to the General Data Protection Regulations (GDPR) in respect of data protection and information security.

3.0 Definition

3.1 An information asset can be defined as;

- an operating system
- infrastructure
- business application
- off-the-shelf product
- user-developed application
- records
- information
- IT hardware

It will have recognisable and manageable value, risk, content and lifecycles and can range from a basic Excel spread sheet or database to a national system. Within the Fund there are many such systems, both electronic and paper that hold information relating to personal, sensitive personal and commercially sensitive data/information.

3.2 The information asset register is defined as a centralised log of all information that is held by the Fund including but not limited to the nature of the data (i.e. personal or sensitive), what information is held (i.e. names, addresses etc.) but also both electronic and physical locations of the information. This is to assist the Fund with tighter controls over its data and data use leading into the GDPR regulation changes.

4.0 Roles and responsibilities

4.1 The responsibility for the Information Asset Register sits on many levels depending on the action needed.

4.2 Compliance & Risk Team

The Compliance & Risk Team are responsible for the overall maintenance and monitoring of the register. It is their duty to conduct a six month update/review on all areas of the register and update on an ad hoc basis if notified in the period between reviews.

Key actions;

- Promoting information asset awareness throughout the Fund by organising training, awareness campaigns and providing written procedures/guidance that are widely disseminated and available to staff
- Assisting with investigations into breaches of confidentiality or data loss of personal and sensitive information
- Co-ordinate the notifications of such breaches with City of Wolverhampton Council and the Information Commissioner's Office (ICO)
- Develop and maintain the Information Asset Register working with Information Asset Owners (IAO)
- Working with the IAO to help mitigate risks to their information assets

4.3 Strategic Director of Pensions (Accountable Officer)

The Strategic Director of Pensions has overall accountability and responsibility for the Information Governance of the Fund and is required to provide assurance that all risks to the Fund, including those relating to information, are managed and mitigated effectively.

4.4 Head of Governance

It is the role of Head of Governance to ensure and act as an advocate for Information Governance including security on the senior management team, which feeds into the Pensions Committee in the Fund's governance structure.

Key actions;

- Provide advice and support for the Pensions Committee and senior management team (SMT) on the Annual Governance statement in relation to information risks
- Liaise with Information Asset Owner (IAOs) on resolution and/or discussion of issues along with Compliance
- Ensure the Fund has a plan to monitor and achieve set requirements for Information Governance, including the culture of the Fund activities and staff
- Approve all information asset areas of the Business Continuity Plan with SMT

4.5 Information Asset Owners (IAO) – Senior Management Team

Information Asset Owners or Senior Management Team is responsible for overseeing the Information Asset Administrators (IAA, or individual staff members) of their management areas.

Key actions;

- Lead and promote a culture of high standards of Information Governance in the Fund
- Know what information is contained in the asset including any additional or removed information
- Know who has access to the asset and why, including access levels if part of an electronic system
- Understand the risks to the asset and able to provide assurance to the SIRO and SMT that data is secure and in the event of a breach understand the reporting cycle
- Ensure that all new assets within their department are reported to Compliance for inclusion in the register along with a completed privacy impact assessment
- Any changes to the asset are documented on the register and follow the correct change procedures
- Any assets destroyed are notified to Compliance & Risk for recording on the register and follow the correct retention policy

- Liaise with Compliance & Risk to ensure that procedures and controls are in place to ensure the integrity and availability of the information assets
- Provide updates to Compliance & Risk and Pensions Committee when required as part of the Compliance Monitoring Programme

4.6 Information Asset Administrators (individual staff)

Information Asset Administrators (IAA) are usually the staff members who understand and are familiar with the information assets in their area.

Key actions;

- To maintain the general data quality of their information asset and report any areas of concern to the IAO
- Ensure that personal or commercially sensitive date is not unlawfully exploited
- Recognise any potential or actual security incidents and consult Compliance & Risk or SMT
- Under the direction of Compliance & Risk, ensure any asset to be destroyed is done so securely when no longer required
- Ensure compliance with data sharing agreements
- Ensure appropriate access to information assets and report any issues that may occur
- Informing Compliance & Risk of any new information asset ort amendments as per the IAO for the area

4.7 All staff

Need to be aware that confidentiality and security of information includes all information relating to members, employers, administering authority, third parties and employees. Such information may relate to staff or member/employer records, electronic databases or methods of communication containing personal identifiable information including mobile devices. Staff will be expected to:

- Read and comply with the Confidentiality agreement which forms part of their contract of employment;
- Adhere to the Data Protection Act Policy and any associated procedures/guidelines;
- Attend all mandatory training and awareness programmes;
- Ensure that all personal identifiable information is accurate, relevant, up-to-date and used appropriately on both electronic and manual records and devices;
- Share information on a ‘need to know’ basis only

- Ensure that all personal identifiable information is kept safe and secure at all times and in line with the Fund's Retention policy;
- Be aware that personal and sensitive information should not be published on the Fund's website.
- Ensure they report any incidents and or events that could have an impact on the information asset; this can be done through the incident reporting procedure.

It must be stressed that you must not take personal identifiable and/or sensitive data home with you or keep it at home unless authorised to do so. No personal identifiable and/or sensitive data is to be stored on your home computer. Home computers can be easily compromised putting all the information at risk. If as an employee you are found to have made an unauthorised disclosure you may face disciplinary action, which could lead to your dismissal and legal action being taken against you. However, where homeworking rules apply, individual officers are responsible for the security and confidentiality of Fund data/information assets. Reasonable steps must be taken by an individual as detailed in the homeworking policy to give assurance back to the Fund that our data is safe and will not be misused in any circumstances.

5.0 Critical Information Assets

5.1 A critical information asset is one which the Fund is reliant on and cannot operate without. The result of the asset being unavailable for a period of time will/could disrupt the service and operation of the Fund's activities. All critical information assets are referenced in the Business Continuity Plan along with the associated timescales. The Business Continuity Plan details step by step procedures to ensure that in the event of no access to the offices etc. the Fund can continue with its required tasks without major disruption to its customers and to meet its liabilities of paying pensioners. Officers must ensure that the critical information assets listed on the register are updated and reviewed regularly so no issues arise with the location or identification of critical assets if the business continuity plan has to come into force.

6.0 Change Control

6.1 Any major changes to information assets must be agreed by SMT, this includes new and or replacement software, system updates and installations, removal or archiving of an information asset and the creation of a new information asset.

6.2 A privacy impact assessment should be carried out whenever a new project or information asset is likely to involve a new use (i.e. data to be used for a task

that it was not originally collected for) or significantly change the way in which personal data is handled.

6.3 All software installations or updates and new hardware equipment must be communicated to City of Wolverhampton Council ICT department and Compliance & Risk team where appropriate. A separate register of physical ICT assets is held by the Technical Team at West Midlands Pension Fund and is maintained regularly.

7.0 Business Continuity

7.1 Business continuity is a core component of corporate risk management and emergency planning. Its purpose is to counteract or minimise interruptions to an organisation's business activities from the effects of major failures or disruption to its information assets (e.g. data, data processing facilities and communications).

7.2 Approved Business Continuity Plans are in place for all critical information assets and all staff are aware of their roles and responsibilities. Information Asset Owners have implemented approved procedures and controls for their information assets and have effectively informed all relevant staff.

7.3 Business Continuity Plans, and system specific procedures and control measures are regularly reviewed, and where necessary tested, to assess their ability to meet their business objectives. It is the responsibility of all officers to be aware and note any changes to the plan before they occur.

7.4 All Business Continuity Plans are to be completed by the Compliance & Risk team and signed off for approval by SMT and Pensions Committee.

8.0 Training

8.1 Information Governance training is mandatory for all staff on induction and on a yearly basis. The Compliance & Risk Team work with line managers to ensure that additional training is available, as appropriate to support staff.

8.2 The Information Governance team work with the Caldicott Guardian, Senior Information Risk Officer, Information Asset Owners and the Communications Team to maintain continued awareness of confidentiality and security issues to all (staff and customers) through many forms of communication (including but not limited to staff bulletins, training questionnaires, newsletters, leaflets, posters, web services, etc.)

9.0 Monitoring, Auditing, Reviewing and Evaluation

9.1 The Information Asset Register will be monitored by the Compliance & Risk Team and any changes reported to SMT on a quarterly basis and to Pensions Committee on an annual basis.

9.2 All Information Asset Owners and Information Asset Administrators will be required to review each asset on a six monthly basis and report any changes to Compliance & Risk.