West Midlands Pension Fund

Data Protection Assurance Statement

BASIC INFORMATION SECURITY MEASURES

Basic information security measures include consideration of the following:

2.1 Information Security Management System/Privacy and Data Protection Management System

- Policy
- Governance
- Process/procedures
- Roles/responsibilities
- Assurance process
- Risk Assessment
- Improvement plan

2.2 Physical Security

- The Fund has fit appropriate locks or other physical controls to the doors and windows of rooms where computers are kept.
- The Fund has a policy of physically securing unattended lap tops (for example, by using lockable docking stations for laptops or locking them in a secure drawer or cupboard).
- The Fund does not use removable media, such as removable hard-drives, CDs, floppy disks and USB drives, attached to business-critical assets. It does have a stock of encrypted flash drives for business use only which are password protected and allocated to individuals on a needs only basis.
- The Fund ensures that all business-critical information is removed from the hard drives of any used computers before disposing of them and has in place a contract (which includes provision for data sharing under GDPR) with a reputable company for such disposal.
- The Fund stores back-ups of business-critical information either off-site or via the Cloud which is managed via its business continuity plan.

2.3 Access Controls

- The Fund uses unique passwords, that are not obvious and which meet industry standard for complexity (Note: not birth dates or easily found or guessed information) and change them regularly (Note: preferably at least every three months).

Data Protection Assurance Statement

- The Fund uses passwords that contain letters in both upper and lower cases, numbers and special keys, and are six or more characters in length. No password may be used more than once in a 12 month period
- The Fund ensures that employees don't write down or share passwords and this is monitored by the Compliance team via the clear desk policy and audit.

2.4 Security and Privacy Technologies

- The Fund has attained ISO Compliance certification and operates to this standard in all working practices requiring all contractors and suppliers to conform to this standard.

- Ensure that all computers used have anti-virus software installed, and the virus definitions are updated at least once a week All incoming and outgoing traffic is scanned for viruses, even if it is from a 'trusted' source. At least once a month, computers are scanned for viruses.
- Laptops are issued to individuals with individual access codes preventing the risk of cross contamination of data.

2.5 Awareness, training and security checks in relation to personnel

- The Fund performs integrity checks on all new employees to ensure that they have not misinformed about their background, experience or qualifications.
- All new employees are provided with bespoke data protection training relevant to their role and are required to complete mandatory E-Learning modules on Protecting Information. Managers ensure employees know where to find details of the information security standards and procedures relevant to their role and responsibilities. The Fund's workforce development team keep records of training provided and attended.
- The Fund ensures that employees have access only to the information assets they need to do their jobs. If employees change jobs, the Fund ensures that they do not retain access to the assets they needed for their old job. When dismissing employees, the Fund ensures that they do not take with them any business-critical information.
- Ensure that no ex-employees have access rights to our systems.
- All Employees comply with the code of practice on using social media.

2.6 Incident/Response Management/Business Continuity

- Ensure that employees understand what is meant by a Security Incident. A security incident is any event that can damage or compromise the confidentiality, integrity or availability of business–critical information or systems.
- Ensure that employees are trained to recognise the signs of Security Incidents. These include

    - strange phone requests, especially for information
    - unusual visitors
    - strange patterns of computer activity
    - unusual appearance of computer screens
    - computers taking longer than usual to perform routine tasks

- The Fund ensures that employees receive training on the need to notify anything which may be a sign of a Security Incident and are kept informed as to the identity of the person to whom such notifications should be made.
- Ensure that if a Security Incident occurs, employees know who to contact and how.
- Have in place a plan to assure business continuity in the event of a serious Security Incident (a "Business Recovery Plan"). The plan specifyies:

    - Designated people involved in the response;
    - External contacts, including law enforcement, fire and possibly technical experts;
    - Contingency plans for foreseeable incidents such as:
        - Power loss;
        - Natural disasters and serious accidents;
        - Data compromise;
        - No access to premises;
        - Loss of essential employees;
        - Equipment failure;

- Ensure that the Business Recovery Plan is issued to all employees and is tested at least once a year, regardless of whether there has been a Security Incident.

After every incident when the plan is used, and after every test, re-examine and update the Business Recovery Plan as necessary using the lessons learned.

2.7 Audit Controls/Due Diligence

West Midlands Pension Fund

Data Protection Assurance Statement

The Fund ensures that it has in place appropriate security audit arrangements including:

- Auditing of who has access to its system (in general and in relation to particular types of information)
- Logging of such access to the system; and
- Auditing of compliance with security procedures.

Online Portal

The West Midlands Pension Fund's Pensions Portal is hosted by the Administering Authority, Wolverhampton City Council and complies with their Cyber Security Policy. A copy of the policy is available on the Fund's website at www.wmpfonline.com/dpapolicies

Compliance with Data Protection Law

The Fund complies with all requirements under Data Protection Law.

The Local Government Pension Scheme ("**LGPS**") in England and Wales is an occupational pension scheme registered under section 153 of the Finance Act 2004 and its rules are currently set out in The Local Government Pension Scheme Regulations 2013 (SI 2013/2356) as amended ("**LGPS Regulations**").

The LGPS is administered locally by administering authorities which are defined in Regulation 2 of the LGPS Regulations and listed in Part 1 of Schedule 3 of the LGPS Regulations.

Wolverhampton City Council ("**Administering Authority**") is an administering authority under the LGPS Regulations. The Administering Authority manages and administers the West Midlands Pension Fund within the LGPS (the "**Fund**") in accordance with its statutory duty under Regulation 53 of the LGPS Regulations.

As it is performing a statutory duty it does not require consent of its members to manage and administer their personal data. More information on how the Fund complies with Data Protection Law can be found in its Data Protection Policy available on our website www.wmpfonline.com/dataprotection.