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

- Data Management Policies
- 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 IT equipment is kept.
  The Fund has appropriate physical controls in place where paper documents that contain personal information are kept.
- 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 password protected flash drives for business use only which are allocated to individuals on a need 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 UK GDPR) with a reputable company for such disposal.
- The Fund stores back-ups of business-critical information on secondary servers either hosted off-site or via the Cloud in a secure manner, which is managed via its disaster recovery planning.

2.3 Technical Security: Access Controls

2.3.1 Passwords

- The Fund ensures users implement unique passwords, that are not obvious, and which meet industry standard for complexity (Note: no words or common phrases from the Oxford Dictionary, nor the current year date can be used), and are changed regularly (Note: high-risk systems will require passwords to be reset every 30 days).
- In line with National cybersecurity advice, the Fund recommends the use of passphrases, e.g., three random words, which are a minimum of sixteen characters and must include the following:
    - letters in both upper and lower cases numbers and special keys.
    - No password may be used more than once in a 12-month period.
    - The Fund ensures that employees do not write down or share passwords with anyone. This is monitored by the Governance, Risk and Assurance team via the clear desk policy and audit.

2.3.2 Access Rights

- The Fund ensures the concept of 'least privilege' is implemented, whereby access to IT systems and equipment is only granted for a user when it is deemed essential by management to their business activities.
- Access rights are reviewed against any changes to an employee's role or responsibilities throughout their period of employment and regular review exercises take place to confirm user lists and their required IT needs.
- Employees that leave the Fund will have their access rights deleted or disabled within five working days of managerial notice.
- An individual can only be issued one laptop which is associated with a unique identifier, this prevents the risk of cross contamination of data via unauthorized access.

2.4 Security and Privacy Technologies

- The Fund's IT infrastructure is hosted by the Wolverhampton City Council, whose cyber security framework is externally reviewed on an annual basis to assess compliance to industry standards, including the Public Services Network (PSN) accreditation and Cyber Essentials Plus certificate.
- The Wolverhampton City Council IT security framework includes:
    - All systems, software and applications used by the Fund being licensed and supported so that they are kept up to date with necessary security updates.
    - Annual penetration testing of Fund hosted websites and portals being undertaken by an independent external party.
    - Daily backups being taken.

- Emails being encrypted, and secure file transfer options are available to securely share personal or confidential information, as required.
- Firewalls being routinely upgraded, and regular network maintenance ensures patching is up to date.
- An external Security Operations Centre (SOC) being in use, to ensure 24/7 security coverage and aid the identification and remediation process for any IT-related security threats.
- All IT equipment is protected by anti-virus software and malware scanning. Device anti-virus is automatically updated daily and cannot be de-activated.
- Each year the Fund reviews and seeks assurance from its suppliers (including the Wolverhampton City Council) to ensure that their IT security and data considerations are still in line with the National cyber security and data protection guidance.

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 and UK GDPR 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 People Services 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 'Acceptable Use of ICT Assets and Social Media' policy, which includes guidance on agile (remote) working and how to manage business-related social media accounts.

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 plans to assure business continuity and disaster recovery in the event of a serious Security Incident ("Business Recovery Plans"). The plan specifies:
    - 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 Business Recovery Plans are issued to all employees and tested at least once a year, regardless of whether there has been a Security Incident.
- After every incident when the plans are used, and after every test, the Business Recovery Plans are re-examined and updated as necessary using the lessons learned.

2.7 Audit Controls/Due Diligence

- The Fund ensures that it has in place appropriate security audit arrangements including:
  - Auditing of who has access to its systems, software and IT equipment (in general and in relation to particular types of information) and when;
  - 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 Information and Cyber Security Policy

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. For further information on how the Fund complies with Data Protection Law please view the Fund's Data Protection Policy that is available on our website: www.wmpfonline.com/dataprotection.