Merseyside Pension Fund

Cyber Governance Policy

Wirral Metropolitan Borough Council

As approved by Pensions Committee on DD MM YYYY following consultation with the Local Pension Board.

Background

Merseyside Pension Fund (the Fund) is one of the largest Local Government Pension Schemes in the UK and manages the pension records of over 150,000 members. The Fund is not a legal entity in its own right but sits as a function of Wirral Metropolitan Borough Council (the Council) who hold the capacity of Administering Authority.

The Administering Authority recognises that cyber-risk is a real and growing threat, and whilst the Council provide the IT infrastructure and computer environment used by the Fund, it remains the responsibility of the Fund to assess the cyber security arrangements of both the internal and external arrangements of the service areas. The Fund is supported in this by rigorous audit processes and checks on an ongoing basis.

Aims & Objectives

The aim of this policy is to set out how the Fund intends to assess and manage cyber-risk and ensure that:

- cyber-risk management and cyber governance are integrated into the overall risk management approach of the Fund to reduce any potential loss, disruption or damage to scheme members, scheme employers or the Fund's data or assets;
- all those involved in the management of the Fund understand cyber-risks and their responsibilities to manage it;
- all data and asset flows relating to Fund operations are identified and evaluated on a regular basis to identify the potential magnitude of cyber-risk;
- there is sufficient engagement with advisers, providers and partner organisations (including the administering authority) so that the Fund's expectations in relation to the management of cyber-risk and cyber governance are clearly understood and are evidenced as part of system & service contracts, and where appropriate regular review by Fund officers;
- an incident response plan is maintained, and regularly reviewed and tested to ensure any incidents are dealt with promptly and appropriately.

Legislation & Guidance

The Fund is required to comply with the provisions of the Occupational Pension Schemes (Governance) (Amendment) Regulations 2018 in relation to the establishment and operation of adequate internal controls to ensure the Scheme is managed in accordance with legal requirements.

This includes the data protection legislation which is particularly relevant in relation to the management of Cyber-risk, and the Fund maintains a separate but linked policy on this area:

Data Protection Policy **https://mpfund.uk/dataprotection**

In setting its approach to cyber-risk and cyber governance the Fund has had regard to the Pensions Regulator's General Code of Practice, which has a dedicated section titled 'Cyber Controls' that came into force on 27 March 2024.

IT Section of the TPR code **https://mpfund.uk/generalcode**

The National Cyber Security Centre, which is part of the Government Communications Headquarters (GCHQ), provide best practice cyber guidance, training, and early warnings of cyber-threats for the

most critical organisations in the UK. The administering authority and the Fund have access to these materials and tools to support day-to-day operations and infrastructure developments.

https://www.ncsc.gov.uk/section/about-ncsc/what-we-do

Review

This policy will be reviewed on an annual basis by the Fund, and in line with the Council's adopted programme of formal review for Cyber Security and Governance. If there is a required change to the policy, the Wirral Pension Board will be asked to consider a revised draft prior to final approval and ratification by Pensions Committee.

Statement of Cyber-Risk

The Fund in its day-to-day operations holds and has responsibility for a large amount of personal data and financial assets which would make the Fund a potential target for cyber criminals. Some of the workings of the Fund is outsourced to third-party providers, who may offer 'cloud-based' or hosted software. As a result, the Fund recognises that a substantial part of managing its cyber-risk therefore means managing the cyber-risk of these third-party organisations.

As well as deliberate cyber-attacks the Fund acknowledges that it is also exposed to accidental damage from cyber threats, including cyber-vandalism, such as the changing of website content or stopping essential services that would hamper the operations of the Fund.

At a high level, the cyber-risk to be concerned about is anything that damages the Fund or its stakeholders as a result of the failure of IT systems and processes, including those of Fund advisers, providers and partner organisations. In practice, attention is focussed on a number of key areas:

- Theft or loss of member personal data;
- Theft or loss of financial assets;
- Loss of access to critical systems (e.g. the pensions administration system);
- Reputational impact on the Fund, the Administering Authority and employers;
- Impact on members (e.g. the service scheme members receive).

The Fund also recognises that, in addition to the direct effect of a cyber-attack, there will be indirect effects such as the cost of rectifying any theft or loss of data or assets, meeting any regulatory fines or other financial settlement.

This policy sets out the Fund's approach to the cyber-governance. It includes how it intends to assess and minimise the risk of a cyber incident occurring as well as how officers plan to recover the service should a cyber incident take place.

Cyber Governance

The Fund's approach to cyber governance is to follow an established best-practice model of **Seek, Shield, Solve** and **Review.**

a) Seek

Identify assets and understand and quantify the risk to those assets.

i. The Fund maintains an Information Asset Register that identifies the critical systems and valuable information and data for the successful operation of services. System owners and administrators are clearly identified and are all senior managers of the Fund who understand their responsibilities.

ii. Specific cyber-risk areas are documented in the Fund's Risk Register which is maintained and regularly reviewed by Fund Officers. The Risk Register is considered as a regular item at Pensions Committee and Pension Board meetings.

iii. The Fund's Senior Manager of Operations & Information Governance (who also acts as the Fund's Data Protection Officer) works closely with senior managers of the administering authority's 'Digital, Data & Technology' division in understanding the risks to the IT infrastructure and computer environment provided by the Council. In particular, the risks posed to any shared assets such as email, internet, and corporate systems.

b) Shield

Protect the Fund and its assets from cyber-criminals and cyber-vandals.

i. The Fund's Senior Manager of Operations & Information Governance is the designated individual for ensuring the cyber-resilience framework outlined in this policy.

ii. The Pensions Committee is delegated responsibility for managing the Fund, supported by the Director of Pensions, and therefore they must be satisfied with how cyber-risk is being managed.

iii. The Local Pensions Board assists in ensuring the Fund meets it responsibilities and therefore will have oversight of this Policy.

iv. It is the responsibility of all Fund Officers to comply with this Policy and the supporting conditions of employment, such as the Council's Information Governance Policy and mandatory Cyber-Security and Information Governance training.

v. Cyber-Security and Information Governance training is provided to Pensions Committee and Pension Board members as part of the Fund's training programme.

vi. The Fund will assess all advisers, providers and partner organisations to ensure they have a appropriate arrangements in place to protect themselves against cyber-threats, taking appropriate specialist advice as required. This includes assessing the Council as the administering authority for providing corporate systems and hosting IT systems and services on behalf of the Fund.

vii. Cyber-Resilience is considered as an integral part of any award of contract under the Corporate Procurement Rules of the administering authority. The Fund will also determine how regularly and to what extent further reviews are required with its service providers, with those organisations that pose the greatest risk being reviewed more regularly.

viii. Third-party service providers to the Fund should provide regular reports on any emerging cyber-risks and incidents. This includes working with the administering authority to ensure the Fund's specific requirements are met.

c) Solve

Be able to react and recover quickly in the event of a cyber-attack.

i. The Fund maintains an Immediate Response Plan, which dovetails with that of the administering authority. The Fund's response planning is developed in conjunction with senior managers of the Council's ICT & Digital division. The key liaisons with the administering authority are the Assistant Director of Finance (Digital, Data & Technology), the Head of Digital Ops & Cyber Security, the Service Delivery Manager and the Cyber Security Manager.

ii. The Fund maintains a Contingency & Resilience Plan for Staff, which documents the arrangements in place for staff in the event of an emergency. It identifies the high priority functions that are critical to the overall purpose of the Fund and the third-party partners who are required to ensure business continuity.

iii. The Council's Risk, Continuity & Compliance Manager is consulted when reviewing arrangements around the subject of business continuity planning.

iv. The Fund has agreed with the administering authority that in the event of a cyber incident affecting the Fund, as a critical service, the Council would provide resources to assist and advise in the incident response and business resumption.

v. The Fund will, from time-to-time, assess the possible financial impact of a cyber-incident on the Fund itself and on the administering authority – recognising that in practice the impact is highly variable depending upon the nature of the attack.

d) Review

Check the effectiveness of the controls in place to mitigate the risks (Cyber Resilience)

i. The Fund's approach to managing cyber-risk as outlined in this Policy will be reviewed on a regular basis, including table-top testing of incident response tests of likely scenarios. This will include regular tests of data restoration and failover systems and redundancy arrangements.

ii. Following any significant IT infrastructure or computer environment change, the Fund will liaise with the administering authority on the suitability of the change and any emergent risks or mitigations that align with the change.

iii. Annually, the Fund will request the administering authority to conduct a "cyber penetration test" from a specialist supplier. This external test will utilise many attack vectors to assess the resilience of the IT infrastructure and overall "attack surface" available to Cyber-Criminals.

Supporting Policies & Documentation

Wirral Council Information Governance Policy

This states how the council will manage its information securely and meet its obligations relating to Data Protection and information security compliance regimes. Every Fund employee must be aware of this policy and confirm their understanding annually as part of the Council's mandatory Corporate Governance Checklist.

https://mpfund.uk/infogovpolicy

Pensions Administration Strategy (PAS)

The PAS documents the data and information flows with our employers and contains a section on Cyber-Hygiene, that outlines the requirements and responsibilities of participating employers in regards Cyber-Security.

https://mpfmembers.org.uk/content/riskdocs

Data Protection Policy

This policy document outlines the means to which the Fund handles personal data and the legal basis to which it can exchange that data with employers.

https://mpfmembers.org.uk/content/riskdocs

Privacy Notice & Fair Processing Notice

The Fund publishes these key documents on the main members' website at:

http://mpfund.uk/yourdata

The Privacy Notice explains how the Fund collects, shares and uses the personal data of its members and their beneficiaries.

The Fund is required by law to protect the public monies it administers. The Cabinet Office requires the Fund to participate in a data matching exercise to assist in the prevention and detection of fraud against organisations within the public sector. This is detailed within the Fund's published Fair Processing Notice.

Merseyside Pension Fund
Castle Chambers, 43 Castle Street
Liverpool, L2 9SH

Telephone: 0151 242 1392
Web: https://mpfmembers.org.uk
https://mpfemployers.org.uk
Email: mpfadmin@wirral.gov.uk