WIRRAL

PENSIONS COMMITTEE

18 MARCH 2025

REPORT TITLE:	**CYBER GOVERNANCE POLICY**
REPORT OF:	**DIRECTOR OF PENSIONS**

REPORT SUMMARY

The purpose of this report is to seek approval from Members for the Fund's cyber governance policy.

RECOMMENDATION/S

Pensions Committee is recommended to approve the cyber governance policy attached as Appendix 1 to this report.

SUPPORTING INFORMATION

1.0 REASON/S FOR RECOMMENDATION/S

1.1 The Merseyside Pension Fund ("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 with appropriate levels of oversight by the Pensions Committee.

2.0 OTHER OPTIONS CONSIDERED

2.1 It is important that Pensions Committee has oversight of the Fund's cyber governance policy so no other options have been considered.

3.0 BACKGROUND INFORMATION

Legislation & Guidance

3.1 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.

3.2 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 in on 27 March 2024.

3.3 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.

Review

3.4 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.

Cyber Governance

3.5 As set out in the policy, the Fund's approach to cyber governance is to follow an established best-practice model of **Seek, Shield, Solve** and **Review.**

- Seek - Identify assets and understand and quantify the risk to those assets.
- Shield - Protect the Fund and its assets from cyber-criminals and cyber-vandals.
- Solve - Be able to react and recover quickly in the event of a cyber-attack.
- Review - Check the effectiveness of the controls in place to mitigate the risks (Cyber Resilience).

4.0 FINANCIAL IMPLICATIONS

4.1 Budgetary provision has been made for the processes and controls set out in this policy. The management and maintenance of information technology with its associated requirements is increasingly complex and expensive.

5.0 LEGAL IMPLICATIONS

5.1 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. The Pension Regulator has identified the management of risk as a key objective for pension funds.

6.0 RESOURCE IMPLICATIONS: STAFFING, ICT AND ASSETS

6.1 There are none arising directly from this report. The management and maintenance of information technology with its associated requirements is increasingly complex and expensive.

7.0 RELEVANT RISKS

7.1 As set out in the policy's 'Statement of Cyber risk'.

8.0 ENGAGEMENT/CONSULTATION

8.1 The Fund has engaged with the administering authority's Digital, Data & Technology division' in the preparation of the policy.

9.0 EQUALITY IMPLICATIONS

9.1 There are no equality implications arising from this report.

10.0 ENVIRONMENT, BIODIVERSITY AND CLIMATE CHANGE IMPLICATIONS

10.1 There are none arising directly from this report.

11.0 COMMUNITY WEALTH IMPLICATIONS

11.1 There are none arising from this report.

REPORT AUTHOR: **Peter Wallach**
(Peter Wallach, Director of Merseyside Pension Fund)

APPENDICES

Appendix 1- Cyber Security Policy

BACKGROUND PAPERS

CIPFA: Managing Risk in the Local Government Pension Scheme
The Pensions Regulator's General Code of Practice
The National Cyber Security Centre
The Fund's Data Protection Policy **https://mpfund.uk/dataprotection**
IT Section of the The Pension Regulator's code **https://mpfund.uk/generalcode**
The National Cyber Security Centre, which is part of the Government Communications Headquarters (GCHQ), provide best practice cyber guidance,
https://www.ncsc.gov.uk/section/about-ncsc/what-we-do

TERMS OF REFERENCE

This report is being considered by the Pensions Committee in accordance with Section A of its Terms of Reference:

(d) To monitor the Local Government Pension Scheme including the benefit regulations and payment of pensions and their day to day administration and to responsible for any policy decisions relating to the administration of the scheme.

SUBJECT HISTORY (last 3 years)

Council Meeting	Date