Isle of Wight Council

Isle of Wight Pension Fund
Cyber Security Policy

February 2025

FOR PUBLICATION – CORPORATE POLICY

1. Document information

Title	Isle of Wight Pension Fund Cyber Security Policy
Status	FINAL
Current Version	V1.0
Author	Steve Harrison Financial Services, Resources Directorate Steve.Harrison@iow.gov.uk
Sponsor	Chris Ward Director of Finance and section 151 Officer chris.ward@portsmouthcc.gov.uk
Consultation	ICT Pension Services Hymans Robertson LLP Local Pension Board
Approved by	Isle of Wight Council Pension Fund Committee
Approval date	5 February 2025
Review frequency	Every three years
Next review	2028

Version Control

Version	Date	
1.0	5 February 2025	Approved by the Pension Fund Committee

Isle of Wight Council

2. Contents

3. Purpose of Policy

3.1. This document has been prepared by Isle of Wight Council (the Administering Authority, or "we") in its capacity as the administering authority of the Isle of Wight Council Pension Fund (the Fund). The Administering Authority recognises that cyber risk is a real and growing threat, and the aim of this policy is to set out how the Fund intends to assess and manage cyber risk.

4. Introduction

4.1. Cyber risk (as defined by the Pension Regulator Cyber security principles for pension schemes, December 2023) can be broadly defined as the risk of loss, disruption, or damage to a scheme, or its members associated with using information technology. Risks can arise not only from the technology itself but also from the people using it and the processes supporting it. It includes risks to information (data security) as well as assets, and both internal risks (for example, from staff) and external risks (such as hacking).

4.2. This Cyber Security Policy applies to the Fund. It is acknowledged that the Council has a dual role as the Administering Authority as well as a provider of shared ICT services to the Fund. It is also recognised that it is the responsibility of the Fund to assess the cyber security arrangements of both the internal arrangements and external arrangements to ensure they are fit for purpose.

4.3. It is recommended that this policy be read in conjunction with the business continuity arrangements for the Fund (including disaster recovery), data breach incident reporting policy and anti-fraud procedures.

5. Aims

5.1. In relation to cyber security, the Fund aims to 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 Fund responsibilities in helping to manage it;
- all data and asset flows relating to the Fund 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 assurance is gained on how those organisations are managing those risks; and

- a cyber incident response plan is maintained, and regularly tested, to ensure any incidents are dealt with promptly and appropriately with the necessary resources and expertise available.

6. Legislation

6.1. The Fund is required to comply with the provisions of the Public Service Pensions Act 2013 and Pensions Act 2004 in relation to the establishment and operation of adequate internal controls to ensure the scheme is managed in accordance with the legal requirements. This includes data protection legislation and in particular, responsibilities under Data Protection Act 2018, which is particularly relevant in relation to the management of cyber risk.

6.2. In setting this Policy, the Fund has had regard to the Cyber security principles for pension schemes as set out by the Pensions Regulator in their General code of practice that came into force on 28 March 2024.

7. Roles and Responsibilities

7.1. The Fund will assess as part of the Fund's annual review of service providers all advisers, service providers and partner organisations deemed relevant (including the Administering Authority) to ensure they have appropriate arrangements in place to protect themselves against cyber threats, taking appropriate specialist advice as required.

7.2. The Fund will take a proportionate approach to assessing each organisation including advisers, providers or partner organisations, depending on the level of risk they pose to the Fund with the greatest risk being assessed first and with more scrutiny.

7.3. The Fund will ensure all detailed cyber security assessments are carried out by those with relevant expertise.

7.4. The Fund will require regular reports from its advisers, providers and partner organisations on cyber risks and incidents.

7.5. The Fund will determine how regularly and to what extent further reviews are required, with those organisations that pose the greatest risk being reviewed more regularly.

7.6. The Fund will, from time to time, assess the possible financial impact of a cyber incident on the Fund and the use of cyber insurance as a mitigation were deemed appropriate and proportionate.

7.7. The Fund will ensure advisers, providers or partner organisations including the Administering Authority, have appropriate system controls in place and up to date firewalls, anti-virus, and anti-malware products.

7.8. The Fund will ensure data and critical systems including those of advisers, providers or partner organisations are regularly backed up.

7.9. The Fund will ensure that members of the Local Pension Board, Pension Fund Committee and officers involved in actively managing the Fund receive cyber and incident response training as appropriate.

7.10. The Pension Fund Committee has been delegated ultimate responsibility for managing the Fund and the internal controls which therefore includes ensuring it is satisfied with how cyber risk is being managed and that the Pension Fund Committee knowledge of understanding of cyber risk is maintained.

7.11. The Pension Board assists in ensuring the Fund meets its responsibilities and therefore has oversight of this Policy as well as responsibilities to ensure that the Local Pension Board's knowledge and understanding of cyber risk relating to the Fund is up to date.

7.12. The Strategic Manager: Pensions is the officer responsible for day-to-day implementation of the new cyber security policy, although ultimate responsibility lies with the Director of Finance & s151 Officer who is the designated individual responsible for the cyber resilience framework outlined in this Policy.

7.13. It is the responsibility of all Fund Officers to comply with this Policy. Fund advisers, providers and partner organisations will be made aware of this Policy and should provide regular reports on cyber risks and incidents. This includes working with the Administering Authority to ensure the Fund's specific requirements are met.

8. Cyber Risk Identification

8.1. The Administering Authority for the Fund holds and has responsibility for a large amount of personal data and financial assets which makes the Fund a potential target for cyber criminals.

8.2. Some of the services of the Fund are outsourced to third party providers. As a result, the Fund recognises that a substantial part of managing their cyber risk therefore means understanding the cyber risk of these organisations.

8.3. As well as deliberate cyber-attacks the Fund acknowledges that it is also exposed to accidental damage from cyber threats. At a high level, the cyber risk is anything that damages the Fund, their members or their employers as a result

of the failure of IT systems and processes, including those of their advisers, providers and partner organisations.

8.4. 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 administration system);
- Reputational impact on the Fund, the Administering Authority and employers; and
- Impact on members (e.g. the service 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 cyber governance. It includes how the Fund intends to assess and minimise the risk of a cyber incident occurring as well as the Fund recovery plans should a cyber incident take place.

9. Cyber Governance

9.1 **Governance:** It is recognised that the Council aligns itself to the ISO/IEC 27001:2022 Information Security Management Systems standard as a widely recognised good practice approach to help provide reasonable assurance of mitigating risks associated with cyber security breaches. A similar standard is also expected from suppliers.

Regular updates are to be provided to the Pension Fund Committee and Local Pension Board regarding the Administering Authorities risk management, data protection and information security frameworks and the appropriateness of the arrangements for the Fund.

9.1. **Training:** Pension Fund Committee members, Local Pension Board members and Fund Officers will receive regular training on cyber risk. The training may cover general cyber risk issues or explore a specific area of cyber risk such as use of devices and home and mobile working. Third party providers will also be expected to provide evidence that their employees receive regular training in relation to cyber risks.

9.2. **Data mapping:** The Fund will use the Fund's Information Asset Register and map where the Fund's data is held (e.g. membership data and on what systems) along with an overview of where and on what systems the Fund's assets are held, (for example with external managers, the Fund's custodian etc.) to document how the Fund's data and assets flow between all the various stakeholders, advisers, providers and partner organisations.

9.3. **Assurance:** The Fund will seek regular assurance from key service providers that they assess and regularly review their attack surface to minimise the range of potential risks and that they regularly monitor any new threats which emerge and request that they advise the Fund when such threats are identified, including any steps to remedy these.

9.4. **Risk Register:** Cyber risks will be documented in the Fund's risk register, which is maintained by Fund Officers and updated on a quarterly basis and reviewed as a regular item at Pension Fund Committee and Local Pension Board meetings.

9.5. **Incident Response Planning**: The Fund has agreed with the Administering Authority that in the event of a cyber incident affecting the Fund, the Administering Authority will provide immediate incident response support and the Fund will be supported by the Council's ICT team including the expertise available via the IWC Cyber Incident Response Team (CIRT), IWC Cyber Security Strategy Programme Board (CSSPB), IWC Information Governance Group ("IGG"), and the IWC Data Protection Office.

9.6. In the event of a cyber incident, The Pension Regulator and other key stakeholders including members and advisors will be informed following any advice from the IWC Cyber Incident Response Team (CIRT) or other advisors as deemed appropriate.

9.7. The IWC Data Breach Incident Reporting Policy will be used to assess data breaches that may need to be reported to the Information Commission Office.

9.8. The Fund will inform all providers, advisers and partner organisations of who needs to be notified when reporting a cyber incident.

10. Review

10.1. This policy will be formally reviewed, at least every three years or earlier if our approach to assessing and managing cyber risk merits reconsideration.

11. Related documents

- Cyber security principles for pension schemes as set out by the Pensions Regulator in their General code of practice that came into force on 28 March 2024
- Business Continuity Plans for the Fund
- IWC Cyber Incident Response Plan
- IWC Data Breach Incident Reporting Policy