Leicestershire Local Government Pension Scheme

Cyber Policy

Sections

Leicestershire County Council as the Administering Authority of the Leicestershire Pension Fund is responsible for setting policies, strategies and statements to ensure the Fund's obligations to its members, employees and stakeholders are met. These are available here.

This policy was approved by the Pension Committee on xx/xx/xxxx.

1 Introduction

The Leicestershire County Council Pension Fund holds personal information for in excess of 100,000 members and has a Fund value of over £5bn. Pension schemes hold large amounts of personal data and assets which can expose them to significant risks if an error occurs. These risks include service disruption, fraudulent activity and data leakage.

The Pensions Regulator requires pension schemes to take steps to build 'cyber resilience' – the ability to assess and minimise the risk of a cyber incident occurring, but also to be able to recover when an incident takes place. Schemes are required to work with all relevant parties to define their approach to managing this risk.

The Pensions Regulator summarises it's expectation of pension schemes as follows:

- Trustees and scheme managers are accountable for the security of scheme information and assets.
- Roles and responsibilities should be clearly defined, assigned and understood.
- You should have access to the required skills and expertise to understand and manage the cyber risk in your scheme.
- You should ensure sufficient understanding of the cyber risk: your scheme's key functions, systems and assets, its 'cyber footprint', vulnerabilities and impact.
- The cyber risk should be on your risk register and regularly reviewed.
- You should ensure sufficient controls are in place to minimise the risk of cyber incident, around systems, processes and people.
- You should assure yourselves that all third-party suppliers have put sufficient controls in place. Certain standards and accreditations can help you and your suppliers demonstrate cyber resilience.
- There should be an incident response plan in place to deal with incidents and enable the scheme to swiftly and safely resume operations. You should ensure you understand your third-party suppliers' incident response processes.
- You should be clear on how and when incidents would be reported to you and others, including regulators.
- The cyber risk is complex and evolving, and requires a dynamic response. Your controls, processes and response plan should be regularly tested and reviewed. You should be regularly updated on cyber risks, incidents and controls, and seek appropriate information and guidance on threats.

The Pensions Regulator requires pension schemes to take steps to build 'cyber resilience' – the ability to assess and minimise the risk of a cyber incident occurring, but also to be able to recover when an incident takes place. Schemes are required to work with all relevant parties to define their approach to managing this risk.

Further information and guidance from The Pensions Regulator can be found here.

The Pensions Manager is responsible for ensuring that sufficient controls are in place to minimise the risk of a cyber incident occurring. This policy details the controls that have been implemented. The policy is split into two sections, Systems and Staff.

2 Policy Objectives

The policy objectives aim to ensure the Fund has robust governance arrangements in place, to facilitate informed decision making, supported by appropriate advice, policies and strategies including those by The Pensions Regulator, whilst ensuring compliance with appropriate legislation and statutory guidance.

3 Purpose of the Policy

The policy is designed to provide assurance to the Fund's stakeholders that all appropriate steps regarding cyber security are in place, that the data held is secure and that any risks are well managed.

4 Effective date and reviews

This policy was first presented to the Local Pensions Board on 26th October 2022 and approved by the Pensions Committee on xx/xx/xxxx. The policy will be reviewed by officers annually and will be presented to the Board and Committee if changes are required.

5 Scope

The policy applies to:

- Administrators of the scheme;
- Third parties who store Fund data on their systems.

6 Cyber Issues Relating to Systems where Pensions Data is stored

6a. Heywood Pension Technologies

Heywood are our main system supplier and are responsible for the provision of:

Altair: A database containing all information relating to all active scheme members, plus those members who have left employment, which includes a benefit calculator, workflow, document imaging and Altair Pensioner Payroll. This is the key system used by Pensions as it holds live data used to calculate pension benefits and is updated daily.

iConnect: A web portal that enables employers to upload scheme member data directly into Altair;

Member Self Service: A web portal that enables scheme members to view their pension records, receive secure correspondence and also perform their own pension calculations;

Insights: A reporting tool to enable Officers to write and run complex reports.

Following an Information Security Risk Assessment of Heywood conducted by the LCC Technical Security Officer in February 2020, it was established that the measures and controls agreed during the procurement process were still in place and cyber accreditations held at the time of procurement had been kept up to date.

Going forward Officers will continue to review arrangements on an annual basis, ensuring that the accreditations continue to be up to date, and in addition, annual disaster recovery exercises and cyber security reviews continue to be carried out annually. Copies of the accreditations and reviews are held on Pension records.

The latest versions of the accreditations that Heywood have in place are:

- Cyber Essentials (expires August 2023)
- ISO 14001:2015 (expires 30th November 2023)
- ISO 9001:2015 (expires 19th December 2023)
- ISO 27001:2013 (expires 19th December 2023)

Further Information

Cyber Incidents

In the event of an incident, Officers will notify Heywood via a log on their helpdesk. This would apply regardless of the size and severity of the incident, though it is good practice to follow up the submission of an urgent log with a phone call. The incident will then be investigated by Heywood. Details of the Heywood contact details are also held offline.

Targeted Cyber Attacks

The biggest risk to data are targeted ransomware attacks. Heywood have advised that the following processes are in place:

To protect data from these attacks, the Leicestershire Altair data is backed up separately from the other Altair customers. A daily backup takes place every night, and the data is stored on a backup repository in the Leicestershire's primary datacentre for 7 days. Every night, that night's backup is copied to the Leicestershire's secondary datacentre (the datacentre that is also used to run the Disaster Recovery server from) and on a weekly basis a backup is then stored offline on tape. In the case of a ransomware attack, there is a physical perimeter of where the malware can encrypt and corrupt data. Heywood's backup repositories are offline – as in they cannot be accessed from the internet, and don't have out bound internet access, and so are virtually invulnerable to these kinds of malware attacks.

Heywood also employ an industry standard Antivirus package that is tuned to detect and defend against particular cryptolocker attacks. However, even if someone was able to access the repository and then also manage to get a ransomware malware to run for long enough to corrupt backup data on one of the repositories, there is 7 days of daily, 4 weekly and 2 monthly backups available immediately from the alternate datacentre.

In the unlikely event that both primary and secondary datacentres are targeted and data is lost, there is still the ability to restore to backups stored on physical tapes. However, due to

the nature of offline tape storage being much slower, these backups are limited to monthly restore points.

Officers will need to manually re-enter data from system audit reports that record all data changes during a specified period.

6b. Other Service Providers

The Fund has contracted other service providers to whom Fund data is shared. Officers will ensure that these providers can provide assurances that they will continue to mitigate, manage and report any cyber issues.

This will require officers to ensure ISO accreditations and business continuity plans are up to date, and also obtain assurances that annual cyber checks, e.g. disaster recovery exercises and penetration testing have taken place. This can be done by obtaining documentary evidence e.g. certificates, reports or emails confirming that checks have been performed.

6c. LCC Network

Officers access the Fund's systems including access to emails through the LCC network. Loss of access to the network would cause significant difficulties in accessing the Fund's systems. The network is managed by LCC and Officers will ensure on an annual basis that regular cyber checks continue to be carried out.

7 Cyber Issues Relating to Staff

7a. Training

In accordance with LCC policy, all staff must undertake mandatory training through LCC's online 'Learning Hub'. This includes cyber related courses including Information Security and Fraud Awareness.

This must be completed within four weeks of joining LCC.

7b. Emails

Emails must be sent safely in accordance with LCC guidance.

7c. **Passwords**

Wherever possible, LPF will comply with the LCC password policy. Where this is not possible, such as PING where the parameters are set by the system administrators, then LPF will adopt the strongest possible parameters within the limits of that system.

<u>Password Policy for Altair</u>

PING

PING is an authentication platform which allows access to altair. Whilst they do not entirely comply with LCC password policy, when combined with the requirement for a secondary login, Officers are satisfied that the security is at an appropriate level.

Altair

Altair is the core administration system used by Pension Officers.

The Fund has adopted the following settings:

A password strength of 7 (very strong);

No expiry date on the password;

Password retry: 9 attempts (LCC [policy allows 10 but Altair limits this to 9)

Minimum password length: 10 characters

Number of stored historic passwords: 8 (these cannot be reused)

These have currently been set to comply with LCC password policy.

Altair allows for the creation of specific roles within it's framework to limit users access to certain functionality within the system.

There are currently five roles used by pensions staff:

Officers	**Role**
Pensions Assistants and Officers	LCC Role 1
Officers who deal with I-Connect	LCC Role Systems Admin
Pensions Officers - Continuous Improvements Team only	LCC Role 3
Assistant/Managers who authorise payments	LCC Role 3 & Authorise
Systems Managers	LCC Admin & Payroll Superuser

In addition, there are two roles used by payroll staff:

Officers	Role
Payroll Officers (input data)	LCC Payroll
Payroll Control Staff (run payrolls)	LCC Payroll Control

Roles are amended as jobs change and a check is carried out every six months, to ensure all users are still on the correct role and leavers have been disabled. In addition a System Audit is also conducted by Internal Audit on an annual basis as part of their key ICT controls work.

7d. Data Breaches

In the event of a data breach, e.g. personal information sent to the wrong scheme member, Pension Officers must follow the LCC procedure, which requires the incident to

be reported via the Incident Reporting Form. This is then sent to the Information Governance Team who will advise on appropriate action to be taken.

The Fund has a Retention Schedule and also a Fair Processing Notice, which specifies how long data can be held and who it is shared with. These documents are reviewed every two years.

7e. Roles and Responsibilities

Activity	Responsibility
Reporting Cyber Breaches	All
Maintaining a Cyber Security Policy for Pension Fund	Pensions Manager and Pensions Project Manager
Reviewing Cyber Risks	Pensions Project Manager and Third Parties
Maintaining Cyber Risks on Pension Fund Risk Register	Pensions Manager
Maintenance of Security Controls on Fund Administration system	Pensions Project Manager
Maintaining Cyber Risk across Administering Authority	LCC Technical Security Officer
Reporting Data Breaches and Incidents	All

8 Officers to Contact

Ian Howe Pensions Manager ian.howe@leics.gov.uk

Stuart Wells Pensions Projects Manager stuart.wells@leics.gov.uk