Leicestershire Local Government Pension Scheme

Cyber Policy

Sections

1. Introduction
2. Policy objectives
3. Purpose of the policy
4. Effective date and reviews
5. Scope
6. Cyber issues relating to systems where pensions data is stored
7. Cyber issues relating to staff
8. Data breaches
9. Cyber roles and responsibilities
10. Further information
11. Officers to contact

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 on the pension fund's website.

This policy was approved by the Pension Committee on 18th November 2022.

The policy was reviewed in December 2024, approved by the Local Pension Committee and this version became effective from XX XXX 2025.

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 (TPR) 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.

TPR summarises its 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 resume operations swiftly and safely. 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.

TPR 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.

Significant cyber incidents must be reported to TPR at: report@tpr.gov.uk . Significant incidents are likely to result in:

- A significant loss of member data
- Major disruption to member services
- A negative impact on a number of other pension schemes or pension service providers

Further information and guidance from TPR can be found on their website.

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 18th November 2022.

This version was approved by the Pensions Committee on DATE.

The policy will be reviewed by officers biennially 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.

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.

Further Information

System Backup Process

Database and full server backups are taken nightly on each hosted Altair server.

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.

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.

Officers purchased two products from South Yorkshire Pension Fund: DART, a reporting tool that uses selected data directly extracted from Altair to produce simple results and EPIC, a database that stores documents and information related to scheme employers, e.g. contact details and discretionary policies. Both are hosted on the LCC network. South Yorkshire officers have approved 'third party sign-in' to access these systems, which is the agreed LCC ICT method for external users to access internal databases.

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.

New staff will also receive a basic overview on Altair before being issued with a username and password.

7b. Emails

Emails must be sent safely in accordance with LCC guidance. Sensitive data must be encrypted, typically using Egress before sending to external recipients.

7c. **Passwords**

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

Altair Roles

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

There are currently seven roles used by pensions staff:

Officers	Role
Pensions Assistants and Officers	LCC Role 1
Pensions Assistants dealing with 'bulk calculations'	LCC Role 1 – with Bulk Calcs
Pensions Assistants checking 'APC's	LCC Role 1 – Checking APCs
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 three roles used by payroll staff:

Officers	Role
Payroll Officers (input data)	LCC Payroll
Payroll Control Staff (run payrolls)	LCC Payroll Control
Payroll Service Desk	LCC Service Desk (Read-Only access)

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.

Any requests to change a user's role must be submitted by email to the Continuous Improvements and Systems Team.

In addition, a System Audit is also conducted by Internal Audit on an annual basis as part of their key ICT controls work.

System Restrictions

Users are forbidden from accessing their own Altair records.

8. 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.

9. Cyber 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

10 Further information

The Fund complies with LCC policies in respect of use of mobile devices (Personal Use of Work Mobile Phones Policy and Bring Your Own Phone policy) and working from home (Smarter Working Policy).

11 Officers to Contact

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

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