Staffordshire Pension Fund
Local Government Pension Scheme

Cyber Security Strategy

October 2023

This Cyber Security Strategy will be revised and republished following any material change in policy.

Cyber Security Strategy (CSS) Background

The Staffordshire Pension Fund (the Fund) holds a large amount of personal data and assets which can make it a target for fraudsters and criminals. Everyone: our members, our scheme employers, and other Fund stakeholders, should be able to feel that their data and the Fund's assets are safe.

Cyber security is the discipline dedicated to protecting information and the systems used to process or store it. A cyber-attack could have very serious consequences, not only in terms of disrupting services but also because of the reputational damage it might cause. And there is also the potential for financial repercussions or some wider impact on individuals in the future.

Cyber security is fast moving, and the challenges and risks of breaches have never been higher, there are an increasing and alarming number of cyber security attacks on government organisations with catastrophic effects on operations and reputation. Increasingly the Fund will have to become even more proactive and more sophisticated in the battle against such threats.

Cyber security will see many developments including, but not limited to, a move towards biometrics for authentication, resulting in a decrease in the reliance on traditional passwords.

"Zero Day" threats, which take advantage of a security vulnerability that does not have a fix in place, will become more common and a robust process for monitoring alerts and incidents across our partners networks will be increasingly important. We will need to work closely with them and external experts in the use of advanced technologies to detect and mitigate technological and cyber risk.

A culture will be developed where staff have the skills and confidence to remain safe while working on-line, both in work and in their private lives.

Strategy Purpose

The purpose of this Cyber Security Strategy (CSS) is to provide assurance to members, scheme employers, and other stakeholders about our commitment to deliver robust information security measures to protect their data and the Fund's assets from misuse and cyber threats. We will also aim to safeguard their privacy through increasingly secure and modern information governance and data sharing agreements with our partners.

Through delivery of the CSS, we have assessed ourselves against:

- Pension and Lifetime Savings Association Cyber Risk Guide; and
- The Pensions Regulators' Cyber Security Principles for Pensions Schemes.

Cyber Security Strategy Scope

This CSS applies to all the Fund's employees, scheme employers, contractors, suppliers, and anyone else who may have access to the Fund's systems, software, and hardware.

This CSS applies to all information and data held or owned by the Fund, any ICT equipment and infrastructure used, and the physical environment in which the information and/or supporting ICT is used.

Where access is to be granted to any third party (e.g. contractors, service providers and partners) compliance with this CSS is assumed to be agreed.

This CSS links into several existing Staffordshire ICT policies and does not replace these documents.

Staffordshire County Council

As the Administering Authority and our largest partner, Staffordshire County Council and Staffordshire ICT are responsible for documenting and maintaining a wide range of technical standards in line with Security Best Practice and Government Guidelines including the ISO 27001 ISMS standard which will be used to identify any gaps in the Council's Cyber Security documentation suite.

These will include standards for:

- Data Security
- System Security
- Resilient Networks
- Identity and Access Controls
- Staff Awareness and Training

Our Roles and Responsibilities

The Pensions Committee is accountable for the security of the Fund's information and assets. Committee Members receive training to ensure they have the skills and expertise to understand and manage the risk.

Cyber Security and the management thereof are identified as a key risk on the Fund's Risk Register, which also focuses on any increases in risks arising from operational changes (e.g. a new system or process).

This CSS is owned by the Assistant Director for Treasury and Pensions supported by the Strategic Investment Manager, the Strategic Pension Manager, and a number of Senior Managers.

Who is Responsible?	For what?
Pensions Committee	• Appreciate and understand the Fund's Cyber Footprint. • Undertake training to ensure sufficient understanding of cyber risk. • Approval of the Fund's CSS. • Engage in incident reporting and rectification.
Local Pensions Board	• Appreciate and understand the Fund's Cyber Footprint. • Undertake training to ensure sufficient understanding of cyber risk. • Assist the Pensions Committee and Administering Authority in developing and reviewing the Fund's CSS. • Engage in incident reporting and rectification.
Director of Finance and Senior Management Team	• Oversee the Cyber Security Risk of the Council and the Pension Fund • Ensure Cyber Risk is covered by Fund policies. • Ensure the Fund has effective controls and a framework in place to protect the security of the Fund's information, data, and assets.
Assistant Director for Treasury & Pensions	• Owner of the Fund's CSS • Oversight of the Fund's Cyber Footprint Register (CFR) and its annual review. • Ensuring the development of a third-party system providers testing programme, in consultation with Staffordshire ICT. • Oversight of the assurance / compliance by other stakeholders and third-party system providers. • Ensuring the existence of a robust Business Continuity and Disaster Recovery Plan for Treasury & Pensions. • Ensuring regular reporting to Pensions Committee on cyber security activities and performance against the Testing Programme
Treasury & Pension Fund Management Team	• Assisting with the delivery of the CSS. • Annual review of the CFR and determining RAG ratings.

	• Delivery of the third-party testing programme, on a 3-year rolling basis • Management of mitigating controls for cyber risk and routine testing of Business Continuity and Disaster Recovery procedures. • Recording and reporting of any cyber breaches or issues.
Fund Officers	• Undertake mandatory training to ensure sufficient understanding of the impact of cyber risk. • Awareness of and adherence to the Fund's CSS and office procedures • Reporting of any cyber breaches or issue to the Treasury & Pensions Management Team • Routinely act to protect all data.

Our Approach to Cyber Security

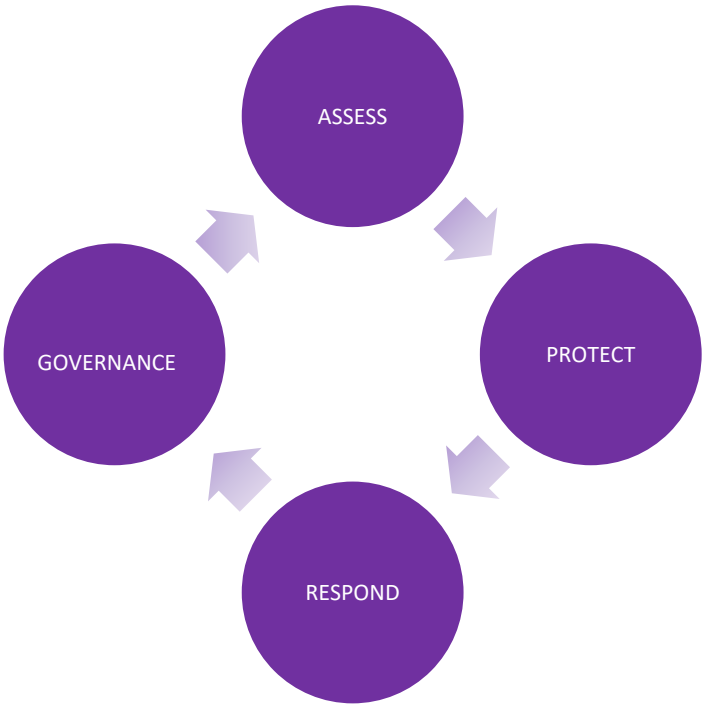
The four main types of Cyber Risk

Type of Risk	Details
Accidental	Loss of hardware (laptop. mobile, USB), loss of electronic data, computer systems failure
Untargeted	Social engineering e.g. phishing exercise which enables malicious content in an email (link/attachment)
Targeted	Deliberate act which can be internal or external e.g. improper use of administrative access or credentials, spoofing, activists etc
Severe	Cyber terrorism and state sponsored attack

Our four stages

We have a four-stage approach to managing cyber security and the risk it poses to the Fund. Our approach focuses on, quantifying the different types of risks (Assess), ensuring effective controls are in place to protect the Fund against those risks (Protect), and ensuring the Fund can respond to a cyber incident if it occurs (Respond). Finally, there is also an appropriate set of policies and procedures that the Fund has in place

around cyber security which ensure everyone is well informed and understands what needs to happen (Governance).



Assess – the risks and understand our vulnerability

We will endeavour to identify, analyse, prioritise, and manage a range of cyber security risks. As part of maintaining our CFR, the Treasury & Pension Fund Management Team will identify, assess, and document the Fund's cyber risks. This will typically include:

- an assessment of our key functions, systems, assets, and dataflows;
- an assessment and detailed mapping of the data flows between the Fund and its partners and third-party providers; and
- an assessment of what we use our data for and the potential vulnerabilities that we may have.

Unless there is any material change or notification of a national cyber security threat, the Fund's CFR will be reviewed at least annually with Red, Amber, Green (RAG) risk ratings assigned to each area of data supplied to the Fund pre and post assurance.

Those suppliers of systems or data perceived to remain of heightened cyber risk to the Fund, be that because of the impact or likelihood of any potential data breach, will be assessed more frequently as part of the

Fund's rolling testing programme. Assessment will be via a cyber security questionnaire developed in conjunction with Staffordshire ICT.

We will also work in collaboration with Staffordshire ICT's Cyber Security Team and the Council's Information Governance Team to ensure we align our priorities and benefit from the sharing of knowledge and experience.

Protect – and safeguard the Fund

Key policies and procedures

A range of Council policies and processes are in place around the acceptable use of devices, email, and the internet (including social media), the use of passwords and other authentication and home and mobile working. Managers are responsible for ensuring that they and their teams are aware of these and comply with their responsibilities under the relevant Staffordshire ICT policies and undertake all identified mandatory cyber risk and information governance training.

Training

It is important that the Fund has the knowledge and skills to understand and effectively manage its Cyber Security Risk. Regular training, in addition to any mandatory training of the Council, will be undertaken by the Pensions Committee and Local Pensions Board, and attendance is monitored by the Assistant Director Treasury and Pensions. As Council Employees, Fund Officers are required to undertake mandatory cyber security training, including annual refresher training, provided by Staffordshire ICT. Where employees do not complete the mandatory training managers are informed and access to the Council's systems may be suspended.

The monitoring of the completion of mandatory training is undertaken by the Treasury & Pension Fund Management Team.

External Suppliers

Cyber security is an active consideration for us when we are selecting suppliers. Assurance is sought from all third-party suppliers that they have the necessary protections in place around our scheme's data and the security of the Fund's assets.

Respond – how we will deal with an incident and Recover

Our ability to react and recover from a cyber security incident or breach is a critical element to managing cyber security. Unless there is any material change, we will carry out an annual review our Business Continuity and Disaster Recovery Plan which details the key steps to be followed,

including the key roles and responsibilities to enable the Fund to resume operations swiftly and safely. This will include:

- **Incident management** – who will oversee, track, report and document the incident?
- **Assessment** – do we understand, the nature, severity, and type of incident?
- **Action** – do we need to implement our Business Continuity and Disaster Recovery plan?
- **Escalation** – communication, who should be notified?

Post-incident review

Following any incident, and as part of the Business Continuity Plan, there will be a structured Debrief which aims to ensure that a detailed analysis is undertaken of the incident itself. This will also include consideration of such things as: the decisions made, communication, costs and expenses and the overall effectiveness of the response, as well as the impact of the incident. Any corrective or preventative actions arising from the Debrief will also be documented.

Governance – documentation and monitoring

The CSS will be listed on the Fund's Governance Register and routinely reviewed, updated, and approved by the Pensions Committee.

The quarterly Risk Register review meetings attended by the Treasury & Pension Fund Management Team will include a discussion and a review of cyber security risks. Cyber Security focussed meetings will be held outside of this as required but will be held at least annually to review the Cyber Footprint Register.

Due diligence checks on perspective suppliers will identify potential cyber security risks. The rolling review of our third-party suppliers on our CFR will ensure that they maintain their standards and any cyber security accreditations.

On an annual basis we will evaluate the Fund's Business Continuity and Disaster Recovery Plan so we are prepared should a cyber security incident occur. This will also incorporate a review of the Incident Log together with any lessons learned from post incident review documents including the Debrief assessments and any Action Log.

Contact us

Assistant Director for Treasury and Pensions – Melanie Stokes
Telephone: 01785 276330
E-mail: melanie.stokes@staffordshire.gov.uk

Strategic Investment Manager – Tim Byford
Telephone: 01785 278196
E-mail: timothy.byford@staffordshire.gov.uk

Strategic Pensions Manager – Simon Jackson
Telephone: 01785 276450
E-mail: simon.jackson@staffordshire.gov.uk

Pensions Systems & Data Manager – Vikki Evans
Telephone: 01785 277163
E-mail: Vikki.evans@staffordshire.gov.uk

Pensions Governance & Communications Manager – Martin Elliot
Telephone: 01785 276278
E-mail: martin.elliot@staffordshire.gov.uk

or by telephoning: 01785 278222

or by e-mailing: pensions.enquiries@staffordshire.gov.uk

We also have a website at: www.staffspf.org.uk

If you would like this information in large print, Braille, audio tape/disc, British Sign Language, or any other language, please ring 01785 278222