Firefighters' Scheme Advisory Board (England)

Cyber Security Policy

Contents

Purpose

The purpose of this policy is to ensure that the Scheme Advisory Board (SAB) maintains effective and proportionate cyber security arrangements to protect the confidentiality, integrity and availability of the SAB website, FPS member website, associated systems and any information processed through them. This policy is designed to align with:

- The Pensions Regulator (TPR) Code of Practice on Governance and Administration (particularly requirements on internal controls, risk management and operational resilience)
- National Cyber Security Centre (NCSC) good practice
- UK GDPR and the Data Protection Act 2018

Although the SAB is not a pension scheme trustee body, it adopts the principles in the TPR Code of Practice as best-practice governance standards.

Scope

This policy applies in respect of:

- The Firefighters' Pension Scheme (FPS) SAB public website and any linked sub-domains
- The FPS member website
- The website hosting environment and supporting services
- Any personal or business information processed via the website (e.g. enquiries, consultation responses)
- SAB members, officers, advisers and third-party service providers with access to the website or its administration. Where confidential data is received through other means, e.g. via emails, SAB members are expected to apply the principles below, in particular in respect of awareness and acceptable use.

Governance and oversight

The Scheme Advisory Board:

- Ensure they have sufficient understanding of cyber risk
- Ensure sufficient controls are in place to minimise the risk of cyber incidents, i.e. risk appetite should effectively be zero except where a risk cannot be mitigated
- Ensure that cyber risk has been considered by Local Pension Boards (LPBs), and third-party providers of services to the SAB.
- Record any incidents and learning therefrom
- Reviews this policy at least annually in accordance with the risk register

Delegated Responsibility

The SAB secretariat is responsible for:

- Day-to-day oversight of cyber security arrangements

- Maintaining contact with website hosting and IT suppliers
- Ensuring incidents are escalated appropriately
- Minimising where possible the amount of confidential personal data supplied to SAB members e.g. by anonymisation of such data

Risk Management

Cyber security risks relating to the SAB website are assessed in a proportionate, risk-based manner, considering:

- Nature of the website (primarily public information)
- Volume and sensitivity of personal data processed
- Reliance on third-party suppliers
- Reputational and service availability impact
- Key cyber risks are recorded in the SAB risk register and reviewed bi-annually.

Data Protection and Information Security

- Personal data processed via the website must comply with UK GDPR principles
- A clear and accessible Privacy Notice must be published
- Data collected must be limited to what is necessary for defined purposes
- All data transmissions must use encrypted connections

Technical and Operational Controls

As a minimum, the following controls will be maintained:

Hosting and Infrastructure

- Secure, reputable hosting provider
- Regular patching of servers and platforms
- Firewall and malware protection

Website Management

- Content Management System (CMS), plugins and themes kept up to date
- Removal of redundant or unused components
- Secure configuration aligned with supplier best practice

Access Management

- Administrator access restricted to named individuals
- Strong passwords and multi-factor authentication where supported
- No shared or generic administrator accounts

Third-Party and Supplier Management

Where third-party suppliers are used (e.g. hosting, development):

- Security responsibilities must be documented in contracts
- Suppliers must confirm compliance with relevant security standards
- Clear incident reporting and escalation arrangements must be in place

Incident Management and Reporting

A cyber incident is any event which compromises, or threatens to compromise, the confidentiality, integrity or availability of the SAB website or associated data.

Incident Response

The SAB will:

- Act promptly to contain and mitigate incidents
- Ensure that there is an incident management team in place, at all times.
- Escalate and continue to inform the SAB Chair of resolution of any significant incidents
- Consider the need to inform users of any incident to the website and deal with any reputational damage
- Involve the LGA Data Protection Officer where personal data may be affected

Regulatory Notification

- Data breaches will be assessed for ICO notification within 72 hours where required
- Lessons learned will be documented and controls improved

Below are the relevant contacts who will form the incident management team.

Role	Contact
Secretariat	firesab@local.gov.uk
Pensions Manager	Clair.alcock@local.gov.uk
Senior Pensions Adviser	claire.johnson@local.gov.uk
Pensions Advisers	Tara.atkins@local.gov.uk Jill.swift@local.gov.uk

Backup, Recovery and Resilience

- Regular automated backups will be maintained
- Backups will be securely stored and periodically tested
- Restoration capability will be reviewed to ensure website availability can be reinstated promptly
- Other secure methods of communication may be used in the meantime

Awareness and Acceptable Use

The SAB website, including the secure area, is provided to support Board business and must be used in a secure and responsible manner. All users share responsibility for protecting information and reducing the risk of cyber security incidents.

SAB Secretariat Responsibilities

The SAB Secretariat, with access to and responsibility for administering the website, must:

- Protect login credentials and ensure that access details are not shared or exposed
- Use secure devices and networks, ensuring appropriate security controls (e.g. updates, antivirus, secure connections) are in place
- Actively monitor and remain alert to phishing attempts, suspicious activity, or unauthorised access
- Ensure appropriate access controls are maintained, including timely removal or amendment of user access where required
- Maintain oversight of the secure area, ensuring documents are appropriately stored and access is restricted to authorised users only
- Document how these requirements are met, and report to the Board annually, or more frequently where necessary, on compliance and any incidents or risks identified

Board Member Responsibilities

All Board members and other authorised users of the SAB website, including the secure area, must:

- Use the website and secure area appropriately, only for official SAB business
- Protect their login credentials and not share passwords or access with others
- Access the website using secure devices and trusted networks only
- Handle all information in accordance with its sensitivity, particularly where documents are confidential or restricted
- Remain vigilant to phishing, suspicious emails, or unexpected system activity, and report concerns promptly to the Secretariat
- Avoid downloading, storing, or sharing sensitive information unnecessarily, particularly on personal devices or unsecured systems
-

Monitoring and review

This policy will be reviewed every two years or at such times as needed by the Board secretariat. The next review will be due in June 2028.

Version Control

Date	Author	Publication	Reason for Change
17/06/2026	Board secretariat	V1	N/A