SCOTTISH BORDERS COUNCIL PENSION FUND

CYBER SECURITY POLICY

People Performance & Change
Pension Fund
Version 2025 1.2
Presented: Joint Pension Fund Committee and Pension Board
11 December 2025

1.Introduction

The Scottish Borders Council Pension Fund (hereafter referred to as “the Fund”) recognises the critical importance of maintaining robust cyber security measures to protect the confidentiality, integrity, and availability of its data and systems. This policy sets out the principles and procedures by which the Fund, part of the Local Government Pension Scheme (LGPS), as administered by Scottish Borders Council, will manage cyber security risks in line with best practice and relevant UK legislation.

Scheme Managers are required by law, under the Public Service Pensions Act 2013 and the Pensions Act 2004, to establish and operate adequate internal controls to ensure the scheme is operated in accordance with scheme rules and the law. Building and being able to demonstrate ongoing cyber resilience is one example of operating adequate internal controls.

2.Purpose

The purpose of this policy is to outline the Fund’s approach to cyber security, ensure the protection of sensitive information, and safeguard the interests of members, beneficiaries, and stakeholders. This policy applies to all employees within the Pensions Administration and Investment teams, contractors, third-party service providers, and any individual or entity with access to the Fund’s information systems.

The Fund recognises that cyber risk is a growing threat. This policy aims to ensure that cyber risk management and cyber governance are integrated into the overall risk management approach of the Fund. This is demonstrated from the inclusion of a specific risk within the Funds Risk Register.

3.Scope

This policy covers all digital assets, systems, networks, and information managed or processed by the Fund, including but not limited to:

- Personal data of pension fund members and beneficiaries
- Financial and investment records
- Communications and correspondence
- Third-party service providers and integrations
- Physical devices and cloud services utilised by the Fund

The Third Party service providers include, but not limited to, the following: -

- Pensions Administration Software provider (Heywood)
- Pensioners Payroll Software provider (Unit 4)
- Strategic IT provider (CGI)
- Scheme Actuary (Hymans Robertson)
- AVC provider (Standard Life)
- Custodian (Northern Trust)
- Investment Advisors (Isio)
- Auditors (Audit Scotland and Scottish Borders Council)
- Overseas Payment provider (Convera)
- Tracing Bureaus (Tell Us Once)

4. Roles and Responsibilities

- Fund Administrator: Overall responsibility for cyber security governance and compliance.
- IT Software Providers: Responsible for implementing and maintaining technical controls and monitoring systems for threats.
- All Staff and Contractors: Required to adhere to this policy and attend regular cyber security awareness training.
- Third Parties: Must comply with the Fund's cyber security requirements as part of contractual obligations.

5. Cyber Security Principles

1. Confidentiality: Information must be protected from unauthorised access or disclosure.
2. Integrity: Data must be accurate, complete, and protected from unauthorised modification.
3. Availability: Systems and data must be accessible to authorised users when required.

6. Security Controls

- Access Management: Access to systems and data is granted strictly on a need-to-know basis. Multi-factor authentication is required for all sensitive systems.
- Password Policy: Strong passwords must be used and changed regularly. Passwords must not be shared or reused across systems.
- Network Security: Firewalls, intrusion detection/prevention systems, and regular vulnerability assessments are in place to protect the Fund's networks.
- Device Security: All devices must have up-to-date anti-malware software, be encrypted where possible, and be secured when not in use.
- Patch Management: Security updates and patches must be applied promptly to all systems and applications.

- Data Protection: All personal and sensitive data must be handled in accordance with the UK General Data Protection Regulation (GDPR) and Data Protection Act 2018.
- Incident Response: All suspected or confirmed cyber incidents must be reported immediately to the Fund Administrator, Information Management Team and IT service provider. See Section 8.
- Backup and Recovery: Regular backups of critical data must be performed and tested to ensure data can be restored in the event of a cyber incident. Documentation and evidence of these having been carried out must be made available to the Fund on request.
- Third-Party Management: Due diligence must be conducted on all third-party service providers to ensure they meet the Fund's cyber security standards.

7. Training and Awareness

All staff and contractors are required to participate in information management, cyber security training and awareness programmes. Additional training will be provided following significant changes to systems or in response to emerging threats.

8. Incident Response

The Fund will develop and test a plan that sets out how the Fund will respond to a cyber incident. This will include the following: -

- The roles and responsibilities of the incident response team and main decision makers.
- Procedures for escalating and responding to incidents.
- System shut down procedures to prevent malware and viruses from spreading.
- Procedures for identifying which systems, data and assets may be compromised, and affected operations and services.
- the priority order for recovering data and services.
- procedures and timescales for recovering backup data and scheme services. Systems and data should only be brought back online when they are secure.
- processes for how and when the trustees will be informed about a cyber incident.
- internal and external communication plans, including to scheme members.
- processes for how and when to report to regulators.

9. Compliance and Monitoring

The Fund will regularly review and audit its cyber security arrangements to ensure compliance with this policy, legislative requirements, and industry best practices. Non-compliance may result in disciplinary action.

10. Policy Review

This policy will be reviewed annually or following significant technological, regulatory, or organisational changes. Updates will be communicated to all relevant parties.

11. Contact and Reporting

All cyber security concerns, incidents, or policy queries should be directed to the Fund Administrator at Scottish Borders Council Pension Fund. Contact details are available on the Fund's website and official communications.

12. Version Control

Version	Nature of Amendment	Date of Change	Author
2025 1.0	Creation of Cyber Security Policy	20 October 2025	Ian Angus
2025 1.1	Amendments following review by Anthea Green	13 November 2025	Ian Angus
2025 1.2	Amended following review by Alistair Langston	28 November 2025	Ian Angus

You can get this document on tape, in Braille, large print and various computer formats by contacting the address below. Ian Angus can also give information on other language translations as well as providing additional copies.

Contact us at Ian Angus, HR Shared Services Manager, Old School Building, Newtown St Boswells, TD6 0SA

01835 826696, iangus@scotborders.gov.uk