SOUTH YORKSHIRE PENSIONS AUTHORITY

September 2024

Data Protection Policy Statement

September 2024

Document Control Information	
Document title	Data Protection Policy Statement
Version	V1
Status	Draft
Owner	Head of Governance and Corporate Services
Department	Resources
Publication date	
Approved by	
Next review date	September 2026

Version History			
Version	**Date**	**Detail**	**Authors**

DATA PROTECTION POLICY STATEMENT

1. Introduction

South Yorkshire Pensions Authority was established on 1st April 1988, following the abolition of South Yorkshire County Council and the winding up of the South Yorkshire Residuary Body. The primary function of the organisation is to administer the South Yorkshire Pension Fund within the Local Government Pension Scheme (LGPS).

The UK General Data Protection Regulation (GDPR) and the UK Data Protection Act 2018 (together referred to as Data Protection Legislation or DPL) regulate the processing of personal data and protect the rights of the data subject.

As the Authority processes personal data, we are registered as a Data Controller (Registration Number Z4920231) with the Information Commissioner's Office (ICO), which means we are responsible for deciding how the data we hold is processed and protecting it from harm.

The Authority regards the lawful and appropriate treatment of personal information as very important to its successful operations and essential to maintaining confidence between the Authority, its employees and its scheme members. The Authority therefore fully endorses and adheres to the principles of the Data Protection Legislation.

2. Purpose and Scope

The purpose of this policy statement is to set out the Authority's commitment to fulfilling its responsibilities to comply with DPL, including how we will apply the seven key principles of data protection and follow good practice in protecting the rights of data subjects.

This document outlines the key roles and responsibilities held within the Authority and the expectations placed on all employees in relation to data protection. It also sets out how this policy statement fits within our Information Governance Framework.

The scope of this Policy Statement applies to:

a. all substantive and temporary employees of South Yorkshire Pensions Authority;
b. any individual including contractors, students / work experience placements and others who work on behalf of the Authority; and
c. elected and co-opted members of the Authority, members of the Local Pension Board and their independent members and advisers.

3. Policy Framework

This policy forms part of the Authority's Information Governance Framework and should be read in conjunction with:

a. Employee Privacy Notice
b. Scheme Member Privacy Notice
c. Data Retention Policy
d. Data Breach Procedure
e. Data Protection Impact Assessment (DPIA) Procedure
f. Information Security Policy

g. Freedom of Information Policy

This policy will be reviewed at least every 2 years or on an ad hoc basis as required in the event of legislative or other changes.

4. Definitions

There are a number of key definitions used within DPL that are relevant to understanding this Policy and the Authority's obligations set out in this policy statement.

Data – means information held in an electronic form (eg. computers, personal organisers, laptops) or information held manually or in paper form as part of a filing system.

A **filing system** means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

Data controller – means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data processor – means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Data protection legislation (DPL) – means the UK General Data Protection Regulation (GDPR) and the UK Data Protection Act 2018.

Data protection officer (DPO) - the individual whose primary role is to ensure that their organisation processes the personal data of its employees, customers, providers or any other data subjects in compliance with the applicable Data Protection Legislation.

Data subject – means an identified or identifiable natural person. Data subjects may include employees, contractors, customers, job applicants, candidates and suppliers; and the data processed may relate to present, past and prospective data subjects.

Personal data – means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Examples of personal data include name, telephone number, age, qualifications and employment history.

Processing – means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Process and processed will be construed accordingly.

Special category data – means racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

5. Data Protection Principles

Article 5 of the DPL sets out seven key principles which lie at the heart of the UK's general data protection regime and to which the Authority is fully committed as part of our approach to processing personal data. These principles in summary are:

a. Lawfulness, fairness and transparency
b. Purpose limitation
c. Data minimisation
d. Accuracy
e. Storage limitation
f. Integrity and confidentiality (security)
g. Accountability

The detail of what these principles require and how the Authority approaches meeting these requirements is set out in the table below.

Principles Personal Data shall be:	The Authority's Approach
a. Processed lawfully, fairly and in a transparent manner in relation to individuals.	**Lawfulness** We have identified an appropriate lawful basis (or bases) for our processing. If we are processing special category data or criminal offence data, we have identified a condition for processing this type of data. We don't do anything generally unlawful with personal data. **Fairness** We have considered how the processing may affect the individuals concerned and can justify any adverse impact. We only handle people's data in ways they would reasonably expect, or we can explain why any unexpected processing is justified. We do not deceive or mislead people when we collect their personal data. **Transparency** We are open and honest, and we comply with the transparency obligations of the right to be informed.

Principles Personal Data shall be:	The Authority's Approach
b. Collected for specific, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historic research purposes or statistical purposes shall not be considered incompatible with the initial purpose.	We have clearly identified and documented our purpose or purposes for processing. We include details of our purposes in our privacy notices for individuals. We regularly review our processing and, where necessary, update our documentation and our privacy notices. If we plan to use personal data for a new purpose other than a legal obligation or function set out in law, we will check that this is compatible with our original purpose, or we will get specific consent for the new purpose.
c. Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.	We only collect personal data that we need for our specified purposes. We have sufficient personal data to properly fulfil those purposes. We periodically review the data we hold and delete anything we don't need.
d. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, is erased, or rectified without delay.	We ensure the accuracy of any personal data we create. We have appropriate processes in place to check the accuracy of the data we collect, and we record the source of that data. We have a process in place to identify when we need to keep the data updated to properly fulfil our purpose, and we update it as necessary. If we need to keep a record of a mistake, we clearly identify it as a mistake. We comply with the individual's right to rectification and carefully consider any challenges to the accuracy of the personal data. As a matter of good practice, we keep a note of any challenges to the accuracy of the personal data.

Principles Personal Data shall be:	The Authority's Approach
e. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; personal data may be stored for longer periods in so far as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.	We know what personal data we hold and why we need it. We carefully consider and can justify how long we keep personal data. We have a data retention policy with standard retention periods where possible, in line with documentation obligations. We regularly review our information and erase or anonymise personal data when we no longer need it. We have appropriate processes in place to comply with individuals' requests for erasure under 'the right to be forgotten'.
f. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.	We have appropriate security measures in place to protect the personal data we hold.
g. The Accountability principle: The Controller shall be responsible for and able to demonstrate compliance with DPL.	We take responsibility for how we handle and process personal data, we ensure that roles and responsibilities are clearly defined and we have arrangements in place to demonstrate our legislative compliance.

6. Roles and Responsibilities

The principal roles and responsibilities in relation to data protection are set out below. Contact details where relevant are included at the end of this policy statement.

Data Protection Officer (DPO)

The DPO:

a. Informs and advises the Authority on its data protection obligations.
b. Monitors the Authority's compliance.

c. Acts as a contact point for data subjects and the ICO.

The DPO has expert knowledge of data protection law and practices and is given sufficient resources and independence to perform their responsibilities effectively.

The role of DPO for the Authority is undertaken by an officer of Barnsley Metropolitan Borough Council (BMBC) under a service level agreement. The officer who fulfils this role is BMBC's Service Director for Customer, Information and Digital Services.

Senior Information Risk Owner (SIRO)

The SIRO is accountable and responsible for information risk across the Authority, and they ensure that everyone is aware of their personal responsibility to exercise good judgement, and to safeguard and share information appropriately.

The SIRO additionally acts as an advocate for information governance and assurance with the Senior Management Team and across the organisation, provides reports to the Authority and to the Local Pension Board relating to information governance and ensures that information risk is taken seriously and actively managed.

The role of SIRO is undertaken by the Authority's Head of Governance & Corporate Services and Monitoring Officer.

Senior Management Team (SMT)

SMT comprises the Director and the Assistant Directors and they are responsible for providing leadership and oversight of the Authority's data protection arrangements. They are responsible for ensuring that a DPO and SIRO are appointed, sufficient resources allocated and that clear responsibilities are identified at a strategic and operational level. They lead by example to promote an organised, proactive and positive approach to data protection that underpins our work.

All Managers and others in a supervisory role

Managers and supervisors are responsible for ensuring that staff in their teams who process personal data in any way:

a. Are made aware of their personal obligations and responsibilities under the current data protection legislation.
b. Receive appropriate training.
c. Are made aware of the Authority's policies and procedures relating to personal information.

All Individuals who have access to Authority data

Individuals who have access to Authority data are responsible for:

a. Complying with the Authority's policies and procedures.
b. Ensuring good data protection and privacy practices are followed at all times.
c. Seeking advice, assistance and training when required.

7. Staff Awareness and Training

Training on data protection is provided to all employees on commencement of employment and the Authority's policies and procedures on data protection are explained as part of the induction process for all new employees during their first month of employment.

Data protection training and awareness of policies and procedures is refreshed for all employees on an annual basis.

The Authority ensures that all policies and procedures relating to information governance are readily available to all staff on the organisation's intranet and that all staff are aware of how to seek further guidance and know when and how to report any actual or suspected data breach.

8. Further Information

Further information regarding our obligations and the rights of our data subjects under Data Protection Legislation is available from the website of the Information Commissioner's Office (ICO) at: Information Commissioner's Office (ICO)

9. Contact Details

Role	Contact Details
Data Protection Officer (DPO) BMBC Service Director for Customer, Information and Digital Services	dpo@barnsley.gov.uk
Senior Information Risk Owner (SIRO) Head of Governance & Corporate Services and Monitoring Officer	informationgovernance@sypa.org.uk