

South Yorkshire Pensions Authority

Data Quality Strategy

DRAFT

<b>Contents;</b>	<b>Page</b>
Introduction	3
Aims and Objectives	3
Legislative and Guidance Requirements	4
Data Covered by the Strategy	5
Effective Internal Controls	5
Protecting Scheme Data	6
Obtaining good quality and timely Scheme data	8
Measuring Strategy Objectives	10
Data Improvement Plan	12
Key risks	12
Reporting	13

DRAFT

## **Introduction**

This Data Quality Strategy outlines the processes and procedures that ensure that South Yorkshire Pension Authority's (the Authority) data is and continues to be of a high quality.

The purpose of the authority is to pay the correct pension benefits to our members when they fall due. It is therefore essential that the Authority achieves and maintains high data quality standards, to comply with its core function and to ensure the cost-effective use of resources. Effectively identifying areas for data improvement and to develop and monitor data action plans where further steps are needed to improve member data. High quality data is also the basis for all fund valuations and effective decision making.

Keeping and maintaining high quality data has become increasingly challenging over time due to the continual diversification of the employer base, increasing numbers of scheme members, employers using external payroll providers and the complexity inherent in the scheme's design. However, the Authority is committed to meeting these challenges by using the approaches outlined in this Strategy. It provides the parameters for assessing areas for improvement based on risk analysis and impact assessment. Through effective risk management the Authority can mitigate the impact of poor data quality, put plans in place to reduce future impact and improve process efficiencies.

This Strategy sets out our approach to protecting, obtaining, monitoring and reviewing our pension scheme data.

## **Aims and Objectives**

### **Our mission:**

To deliver a sustainable and cost-effective pension scheme for members and employers in South Yorkshire delivering high levels of customer service and strong investment returns which facilitate stable contributions.

### **Data Quality Aims and Objectives**

Our key objectives in relation to data quality are as follows:

- Ensure accurate records are maintained to enable the accurate calculation (and payment) of pension entitlements and employer liabilities; ensuring all information and data is communicated securely and accurately, within prescribed timescales.
- To improve member experience of the Authority, providing accurate information at the right time to enable them to make informed decisions about their retirement options.
- Ensure that the Authority is compliant with legislation and with the General Code of Practice and the guidance of the Pension Regulator. Furthermore, in doing so, ensuring we establish a robust, reviewable and transparent

framework necessary for the acquisition and upkeep of accurate, complete and up-to-date records.

- To ensure clarity of roles and responsibilities between the Authority and employers, ensuring all parties are committed to continuing engagement to improve data quality and promote accurate records.
- Establish proportionate, cost effective and efficient data cleansing approaches relative to the particular importance of each data item. As part of this, appropriate technology will be used wherever possible to improve data quality standards, and the streamlining of operational processing across employer and Authority workstreams.
- To ensure data management processes are clearly documented and regularly reviewed.
- To focus on making sure the Authority's data is correct at source by using preventative approaches wherever possible. Data cleansing activities should very much be used as a second line of defence, rather than the main strategy to hold clean data.

## **Legislative and Guidance Requirements**

There are a number of legislative requirements that we must adhere to relating to data quality and record keeping, including but not limited to:

- Local Government Pension Scheme Regulations 2013
- Public Service Pensions (Record Keeping and Miscellaneous Amendments) Regulations 2014
- The Pensions Act (various) including 1995, 2004 and 2008
- Finance Act 2004
- The Occupational Pension Schemes (Scheme Administration) Regulations 1996
- The Occupational and Personal Pension Schemes (Disclosure of Information) Regulations 2013
- Pensions Dashboard Regulations 2022
- Data Protection Act 2018 and the Retained Regulation (EU) 2016/679 (the UK General Data Protection Regulation)
- Freedom of Information Act 2000

In addition, there is a range of guidance relating to data quality and record keeping for pension schemes including:

- The Pensions Regulator's General Code of Practice
- The PASA guidance on Data Management Plans

In developing and implementing this Strategy, we will ensure we adhere to legal requirements and have regard to guidance, prioritising those areas of guidance which have stronger compliance expectations associated with them e.g. The Pension Regulator's General Code of Practice.

## **Data covered by this Strategy**

The Public Service Pensions (Record Keeping and Miscellaneous Amendments) Regulations 2014 set out records that must be maintained by governing bodies of public service pension schemes, including the Local government Pension Scheme (LGPS). We must keep records of:

- scheme member and beneficiary information. Including elements such as name, date of birth, gender, address, national insurance number and specific information relating to their scheme membership
- transactions, including employer and member contributions, pension and benefits payments and any movement or transfer of assets in and out of scheme.

Further requirements are outlined in The Pension Regulator's General Code of Practice Record Keeping, and Data Monitoring and Improvement modules.

As well as storing our data, we receive and send our data to a range of stakeholders including:

- Scheme members
- Scheme employers
- Pension Fund Committee
- Pension Board
- Pension Fund staff
- Pension Fund advisers
- Trade Unions
- Local taxpayers
- Members of the public
- Scheme Advisory Board (SAB)
- The Pensions Regulator (TPR)
- Government departments
- His Majesty's Revenue & Customs (HMRC)
- Ministry of Housing, Communities and Local Government (MHCLG)
- HM Treasury
- Department for Work and Pensions (DWP)

## **Effective internal controls**

Under section 249B of the Pensions Act 2004, we are required to establish and operate internal controls, which are adequate for the purpose of securing that the Authority is administered and managed in accordance with the LGPS regulations and any other legal requirements. In relation to data quality, our internal controls are the systems, procedures and processes we use to ensure we meet the objectives of this Policy, and they are therefore fundamental to how we operate. We are also required to be able to demonstrate to The Pension Regulator (TPR) that we operate processes to maintain accurate and up to date records for the purpose of running the pension fund.

Some of the ways that we ensure our internal controls are robust include:

- having suitably trained pensions staff
- having clear roles and responsibilities for all staff including appropriate authorisation levels
- our staff must undertake mandatory learning on protecting personal data and information governance
- our staff are granted the appropriate level of system access (including external systems, e.g. HMRC's government portal) to fulfil their duties and that access is withdrawn upon the member of staff leaving the team. This minimises the risk of accidental loss, errors and unauthorised activity
- data manually input into systems is subject to a check by a separate and suitably experienced staff member
- all calculations of benefits are subject to authorisation by a separate suitably experienced staff member
- our administration system includes workflow processes to minimise the risk of manual error
- all payments in and out of the Fund are reviewed on a regular basis to ensure they are assigned to the correct accounting codes
- all key internal processes and procedures are documented, and subject to review to ensure they remain appropriate
- our control processes are subject to review by audit and any management actions required in connection with recommendations for improvement are monitored through to completion
- providing appropriate training to employers to ensure they can fulfil their responsibilities

Further information is included later in this Strategy on the various ways that we monitor and review the quality of data we hold.

We also have a separate procedure for Recording and Reporting Breaches of the Law and Late Payment of Contributions by an Employer which may need to be used if the internal controls referred to above have not been met.

## **Security and protecting scheme data**

Our procedures and controls (as outlined elsewhere in this Strategy) have been designed to comply with the Data Protection Act 2018 and the UK General Data Protection Regulation. In addition, we have our own Cyber Security Strategy, which includes several requirements including staff training, cyber hygiene guidance and regular supplier cyber assessments (including relating to our IT systems).

### **How we send data securely**

The Authority's Data security guidelines are followed when sending any personal data.

The main process we use is Egress, to secure and control information sent to third parties, to prevent any sensitive information from being accidentally sent to unauthorised recipients.

We also send data securely to our regular partner organisations and suppliers/advisers by uploading to secure portals.

In relation to data security ahead of the launch of pension dashboards, we have appointed an Integrated Service Provider (ISP) which is a third-party provider responsible for connecting our scheme data with the dashboards' ecosystem. There is no central database within the ecosystem that holds personal information and the ecosystem functions like a giant switchboard connecting users with their pensions via dashboards. To meet data security requirements relating to pensions dashboards a Data Protection Impact Assessment (DPIA) has been carried out with the ISP before connecting to the dashboards architecture. The objective of the DPIA is to identify, communicate and effectively manage any privacy risks concerning the collection or use of personal information.

## **How we receive data securely**

### **Employers and payroll providers**

A key method of data transfer relating to the Authority is the receipt of information from employers in relation to scheme members. All employers are expected to ensure that information that is sent to us containing personal data is sent securely.

In order not to compromise on security, we expect this information to be sent electronically with appropriate encryption and from an Authorised Officer as approved by the employer. Information sent to us without encryption or not from an Authorised Officer can be refused.

### **Scheme Members**

Members can issue data to us in one of three ways; in writing, via email or by uploading information to our member self-service portal.

We emphasise to members that any information being sent to us via email should be sent securely. We also encourage use of the member portal, where available, as this is the most secure and efficient way for data to be sent to us.

### **Third party service providers**

We have several contracts/arrangements in place with third party service providers to help us in our aim of achieving the highest standard of data. Data security and information sharing agreements are covered as part of each service provider contract. Further information on how we work with third party providers is covered below.

## **Data retention**

This Authority has a data Retention Policy in accordance with data protection legislation.

### **Data Protection relating to shared information with employers**

There is no requirement under the Data Protection Act 2018 for data controllers to enter formal contractual relationships with other data controllers with whom they share and from whom they receive personal data. This therefore applies to us and our participating employers.

## **Obtaining good quality and timely scheme data**

### **Employers and payroll providers**

Information is uploaded monthly. It is widely recognised that regular transmission of data dramatically improves data quality.

We monitor the submission of data on a regular basis to ensure all employers are submitting their data in the correct format and in a timely manner. We also have a separate employer escalation policy which will be used to engage with employers who are not meeting our requirements.

The Authority is reliant upon the accuracy, completeness and timeliness of data provision from employers and any third-party agencies they may utilise e.g. payroll providers. All data submissions must be made using the method prescribed. The Authority has a robust induction process for all employers.

To maintain complete and accurate records there needs to be a continual dialogue with employers regarding the provision of data, particularly as employer contacts change. Authority Officers will work with named employer representatives throughout the year, clarifying information and data provided and actively seek to train employers on all aspects of pensions administration as necessary. It is an employer responsibility to both provide accurate data and to provide resources to respond to ad-hoc enquiries, bulk data activities such as monthly data submissions and data reconciliations.

The Authority will set out an employer training plan, review and improve all material available to employers such as the employer's guide and continue to provide other supplementary information through newsletters, forums, the Administration Strategy, the website and webinars.

### **Scheme members**

Various checks are undertaken on data received from members including validations on data maintained online by members and checks against data provided via email or in writing.

### **Working with third party providers**

We work with a number of third-party providers to support us in meeting our objectives. The use of these sources to obtain data form part of our requirement to

monitor scheme data and we use this to check data accuracy when assessing member benefit entitlements. It also supports us in our overall objective to ensure the correct benefits are paid to the correct people at the correct time. Data is therefore obtained and used from the following sources:

### **LGPS National Insurance Database**

The secure National Insurance Database (NIDB) is administered by the Authority on behalf of the Local Government Association. It was developed to allow LGPS administering authorities to share data to prevent duplicate payment of death grants and to identify service in other LGPS funds which may impact benefits in the individual Funds. We use the NIDB as and when required, e.g. where a death grant is payable, to identify eligibility for refunds and aggregations and if “McCloud” qualification may be impacted.

### **Tell Us Once Service**

The NIDB links the membership profile with the Department of Work and Pensions (DWP) ‘Tell Us Once’ service (TUO). The TUO service allows a person registering a death to request that the DWP notifies other government services and council services, including the Authority, of the death. We download notifications from the TUO service daily to ensure payments to deceased members are stopped promptly. In these cases, a copy of the death certificate is not required as the TUO notification is an official notification of death.

### **National Fraud Initiative**

The National Fraud Initiative (NFI) is a biennial exercise that matches electronic data within and between public and private sector bodies to prevent and detect fraud. As a participant, we receive a report of ‘matches’ to investigate, to take remedial actions and update records accordingly.

### **Tracing services**

We use the Department for Work and Pensions to trace addresses for scheme members which is done on a case-by-case basis when required. If we require a larger scale bulk tracing exercise to be carried out, we commission a third-party provider to carry this out considering the scope of the work.

### **Mortality screening**

We commission a third-party provider which carry out a periodic review of our deferred and pensioner membership against the national death register. The purpose of this exercise is to identify members who have died so that the appropriate adjustments to benefits can be made in a timely manner.

### **Overseas pensioner existence checking**

We carry out checks to help us identify when overseas pensioners are no longer entitled to receive benefits.

### **Measuring the Strategy objectives**

We will monitor our performance in achieving the objectives set out in this Strategy by using the following measurements.

Objective	Measurement
<p>To ensure accurate member and transaction records are maintained to support the aims of ensuring the correct benefits are paid to the correct people at the correct time</p>	<p>Common and scheme specific data scores do not decrease year on year.</p> <p>Key Performance Indicators achieved in 90% of cases* (100% for statutory requirements).</p> <p>Data issues are not a significant or moderate cause of delays, inaccuracy, or mistaken identity in pensions administration.</p> <p>All data is available in time for Annual Benefit Statements to be issued by the statutory deadline.</p>
<p>To ensure accurate member and transaction records are maintained to support the aims of ensuring employer liabilities are correctly calculated</p>	<p>Little or no assumptions need to be made by the Scheme Actuary based on missing or inaccurate data.</p> <p>No errors are identified in relation to employer liabilities.</p>
<p>To obtain, store, review and transmit data securely in a cost effective and efficient manner, utilising technology and automation appropriately to obtain value for money</p>	<p>100% of employers use the secure employer hub to provide monthly data returns.</p> <p>100% of data is exchanged with third parties using secure, agreed methods.</p> <p>There are no data breaches or cyber incidents.</p>
<p>To comply with data protection, record keeping and other data quality related legislation as well as aiming to adhere to relevant guidance such as from The Pensions Regulator</p>	<p>There are no data breaches or cyber incidents</p> <p>Evidence compliance with data monitoring and improvement/record keeping modules in The Pensions Regulator's Code</p> <p>Common and scheme specific data scores do not decrease year on year</p> <p>Key Performance Indicators achieved in 100% of cases for statutory requirements</p>

<p>To ensure the roles and responsibilities between the Fund, employers and other stakeholders in relation to data quality are clear and understood</p>	<p>The Pensions Administration Strategy sets out roles and responsibilities</p> <p>Employer escalation procedure in place and when used results in improvement in the timeliness and accuracy of data submitted</p> <p>Annual satisfaction surveys with employers achieving 90% of score in relation to questions about understanding their responsibilities.</p>
<p>To identify and resolve data quality issues quickly, and ensure preventative actions are put in place to reduce the need for future data cleansing activities</p>	<p>Data Improvement Plan in place, which is regularly updated evidencing data issues identified, resolved quickly and preventative actions put in place</p>
<p>To ensure data management processes are clearly documented and regularly reviewed.</p>	<p>All data management processes are stored securely, and all appropriate staff have access to these. All processes are reviewed on an annual basis and a record kept of the review</p>

## Data Improvement Plan

We maintain individual data improvement plans for separate activities, including end of year data cleansing, queries arising from the valuation and Pensions Dashboards projects. We use our inhouse data reporting tool to help us to monitor the presence, quality and format of data and this helps us to determine further steps needed as part of specific data improvement activities.

Based on the output of the data reporting tool we will create a high-level data improvement plan setting out our overall data improvement activities relating to all areas of fund business, should we feel this is required, to support with oversight and monitoring of progress.

We update the separate Data Improvement Plans on an ongoing basis as data quality issues are identified and progress is made in resolving them. The continuous cycle of data analysis ensures the Authority remains committed to ensuring complete data accuracy in the information it holds about its members.

## Key risks

The key risks to the delivery of this Strategy are outlined below. The Assistant Director Pensions and other officers will work with the Authority board and Local Pension Board in monitoring these and other key risks and consider how to respond to them.

- Significant increase in the number of employing bodies causes strain on employer compliance and liaison.
- Employers provide the bedrock of the data requirements for active members. There is a risk of us holding poor quality or missing data due to the failure of the employer to provide the necessary data in a timely manner. We seek to reduce this risk through being proactive with employers, seeking positive engagement with them and providing effective systems and training.
- Failure to maintain employer contact database leading to information being sent to incorrect person
- Significant external factors, such as national change, impacting data requirements and security of data already held (e.g. Pensions Dashboards)
- Failure to maintain records adequately, resulting in inaccurate data resulting in inaccurate member benefit entitlements.
- Due to the technical complexity of the LGPS, it takes time to train staff to the required level and it makes staff retention particularly important. Therefore, there is a risk if the Authority encounters difficulties recruiting and retaining staff.
- Use of external printers/distributors resulting in data mismatch errors
- Linked to the Authority's ever-increasing reliance on software packages, cyber-attacks would have an increased impact on the Fund's ability to operate with an incident leading to loss, compromise, or theft of data.

## Reporting

We will include an overview of our performance against the objectives in this Strategy to Authority Board and Local Pension Board on an annual basis (noting there is some overlap of these measures with our Pensions Administration Strategy which are reported to Local Pension Board quarterly). Further data quality measures such as our common and scheme specific data scores are reported on within our Annual Report and are reported to Pension Board annually.

We also have a separate procedure for Recording and Reporting Breaches of the Law/ Late Payment of Contributions by an Employer. Therefore, if we do not adhere to any legal requirements in relation to the management of scheme data, the matter will be recorded on our breaches log, and where considered to be materially significant, reported to the Pensions Regulator. Furthermore, if a personal data breach occurs along with considering reporting to the Pensions Regulator in line with our procedure for Recording and Reporting Breaches of the Law/Late Payment of Contributions by an Employer, we will record details of the breach and if required we will ensure that we notify the Information Commissioner's Office and/or the member(s).

DRAFT