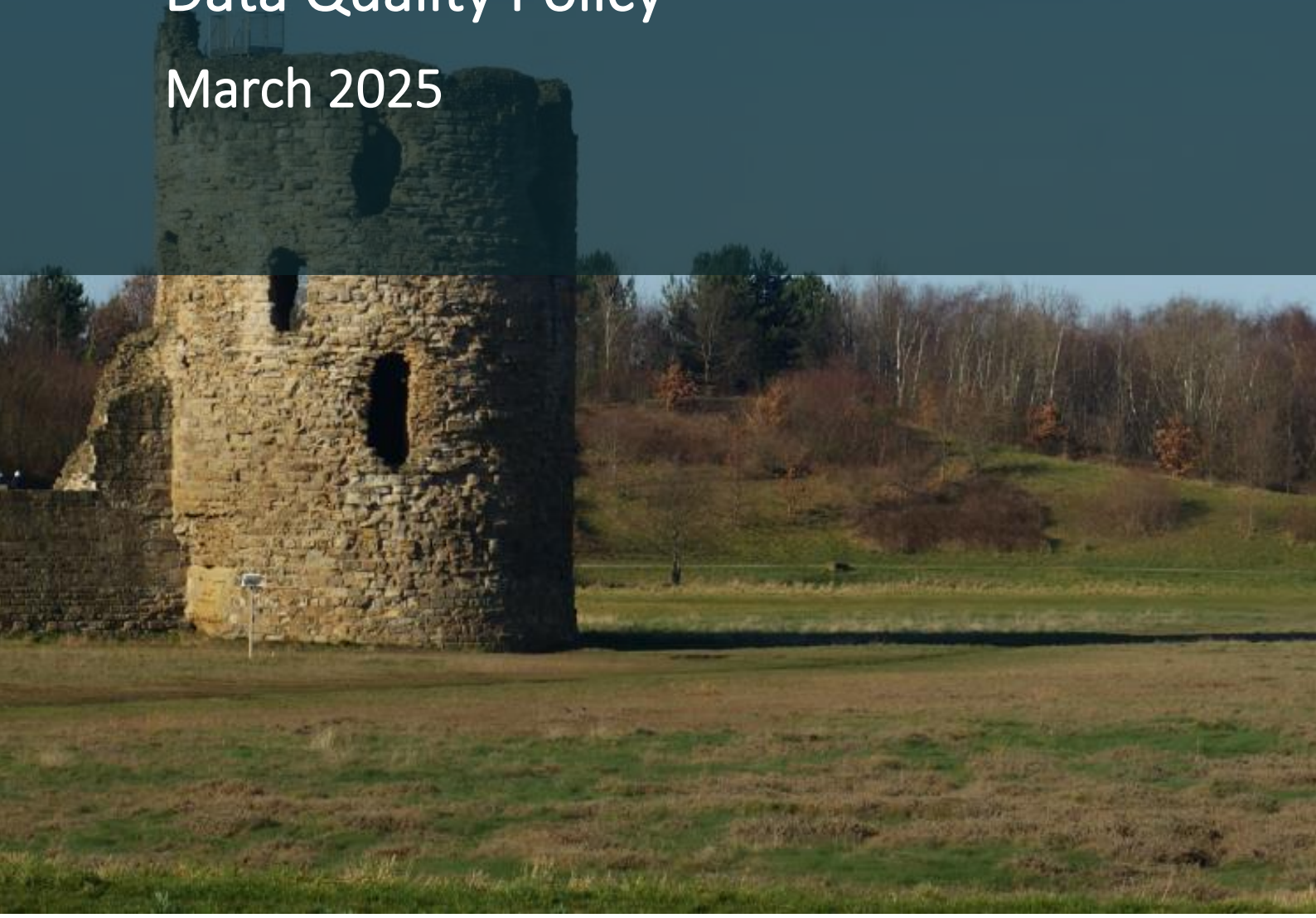


Clwyd Pension Fund

Data Quality Policy

March 2025



Contents

Introduction	3
Aims and Objectives.....	3
Mission Statement	3
Data Quality Aims and Objectives	3
Legislative and Guidance Requirements.....	4
Data covered by this Policy	5
Effective internal controls.....	6
Security and protecting scheme data	7
How we send data securely	7
How we receive data securely	8
Employers and payroll providers	8
Scheme Members	8
Third party service providers	8
Data retention.....	8
Data Protection relating to shared information with employers	9
Obtaining good quality and timely scheme data.....	9
Employers and payroll providers	9
Scheme members	9
Working with third party providers	9
Monitoring and reviewing data: data cleansing activities.....	11
Measuring the Fund against the Policy objectives	16
Data Improvement Plan.....	17
Key risks	17
Reporting.....	18
Approval, review and consultation	18
Further Information	19
Appendix A: Data controllers.....	20
Appendix B: Personal Data Retention Policy	21

Introduction

This is the Data Quality Policy for the Clwyd Pension Fund (“the Fund”). The Policy outlines our processes and procedures for ensuring our data is and continues to be of a high quality. It has been developed following consultation with employers in the Fund, Pension Board members and other interested stakeholders.

Flintshire County Council (the "Administering Authority" and also referred to as the “Governing Body” in this document) is responsible for the local administration of the Fund, which is part of the Local Government Pension Scheme (“the LGPS”). The Fund comprises around 52 employers with active members, and approximately 52,000 scheme members (including active, deferred and pensioner members, and their dependants).

This Policy sits alongside our Pensions Administration Strategy which outlines our overall approach to delivering the highest standard of administration. One of the key objectives in our Administration Strategy, which is driven by overriding legal requirements, is to pay the correct benefits to the correct people at the correct time. High data quality is an essential requirement in meeting this objective, as well as enabling the correct calculations of the Fund’s liabilities to support in effective decision making.

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

Aims and Objectives

Mission Statement

The Clwyd Pension Fund's Mission Statement is:

- to be known as forward thinking, responsive, proactive and professional providing excellent customer focused, reputable and credible service to all our customers
- to have instilled a corporate culture of risk awareness, financial governance, and to provide the highest quality, distinctive services within our resources
- to work effectively with partners, being solution focused with a ‘can do’ approach

Data Quality Aims and Objectives

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

- 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, and employer liabilities are correctly calculated
- 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

- 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
- to ensure the roles and responsibilities between the Fund, employers and other stakeholders in relation to data quality are clear and understood
- to identify and resolve data quality issues in a timely manner, and ensure preventative actions are put in place to reduce the need for future data cleansing activities
- to ensure data management processes are clearly documented and regularly reviewed.

The activities outlined in this Policy will support the Fund in achieving its Administration aims, outlined in the Pensions Administration Strategy.

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 and 2004
- 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 2022¹
- 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 Practice²: in particular, the Record Keeping, and Data Monitoring and Improvement modules
- The PASA guidance on Data Management Plans³
- Pensions dashboards connection requirements and standards⁴

¹ At the time of writing, we have a National Pensions Dashboard Implementation Project underway. This is focussed on setting up the appropriate systems and ensuring our data is of a high quality level for connecting to the National Pensions Dashboard eco-system ahead of dashboards being available to the general public. The date of this (at the time of writing) is still to be announced by Government. This Policy will be reviewed if necessary to incorporate further requirements relating to the National Pensions Dashboards when it is launched.

² [TPR general \(single\) code of practice | The Pensions Regulator](#)

³ [Data Management Plans Guidance – March 2021 – The Pensions Administration Standards Association](#)

⁴ Including but not limited to the Pensions Dashboards Programme standards guidance, DWP's guidance on connection and TPR's Compliance and Enforcement Policy.

In developing and implementing this Policy, 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 (for example, The Pension Regulator's General Code of Practice).

Data covered by this Policy

The Public Service Pensions (Record Keeping and Miscellaneous Amendments) Regulations 2014⁵ set out records that must be maintained by governing bodies of public service pension schemes, including the LGPS. As a governing body, 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)
- Pension Board meetings (including the date, time and place of meetings, attendees and decisions).

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

However, the data required to manage the Fund extends beyond those requirements (for example, records relating to our other meetings such as the Pension Fund Committee.

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

- Scheme members
 - Active
 - Deferred
 - Pensioners
 - Dependants
 - Prospective
 - Other beneficiaries and representatives
- 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

⁵ [The Public Service Pensions \(Record Keeping and Miscellaneous Amendments\) Regulations 2014](#)

- His Majesty's Revenue & Customs (HMRC)
- Department for Ministry of Housing, Communities and Local Government (MHCLG)
- HM Treasury
- Department for Work and Pensions (DWP)
- Audit Wales

This Policy relates to all data we store, send and receive, not just that specifically set out within legislation.

The large majority of our data is the records we hold for scheme members to administer their benefits. Therefore, whilst there are other data and record keeping requirements (such as those relating to keeping records of meetings) the focus of this Policy is on how we maintain high quality member data.

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 Fund 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 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 a check 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 cost centre
- all key internal processes and procedures are documented, and subject to an annual review to ensure they remain appropriate

- our control processes are subject to annual review by internal 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 are able to fulfil their responsibilities

Further information is included later in this Policy 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/ 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 Policy) 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 a number of requirements including staff training, cyber hygiene guidance and regular supplier cyber assessments (including relating to our IT systems).

How we send data securely

We follow Flintshire County Council's data security guidelines when sending any personal data.

The main process we use is Egress Switch, which offers a combination of policy based gateway and desktop email encryption software to secure and control information sent to third parties. Egress Switch also uses:

- an authentication process
- password protection, and
- confirmation of receipt

to prevent any sensitive information from being accidentally sent to unauthorised recipients.

Other ways we send data securely to our regular partner organisations and suppliers/advisers include:

- uploading to secure portals for some of our suppliers/advisers
- utilising a two way secure Transport Layer Security connection

In relation to data security ahead of the launch of pension dashboards, we are required to appoint 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. In order to meet data security requirements relating to pensions dashboards a Data Protection Impact

Assessment (DPIA) must be carried out by the ISP before connecting to the dashboards architecture, and this has been carried out by our ISP, Heywood. 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 Fund's administration 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 to meet the requirements set out in this Policy in a secure and efficient way, we use a secure data system known as i-Connect for our employers. Whilst we expect all employers to use the i-Connect portal to submit information, we recognise that there will be occasions where employers will need to send information to us outside of i-Connect (e.g. prior to the employer being onboarded as an i-Connect user or where supplementary information is required). In these instances, 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 will not be accepted.

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 as this is the most secure and efficient way for data to be sent to us. In some cases where information is uploaded to the member portal the status of a task is updated in the administration system which automatically notifies our team to proceed with the case.

Third party service providers

We have a number of 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

Our Policy on the retention of personal data in accordance with data protection legislation when processing personal data is set out in Appendix A.

Data Protection relating to shared information with employers

There is no requirement under the Data Protection Act 2018 for data controllers to enter into 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. The process around how we and our employers must manage this is set out in Appendix B.

Obtaining good quality and timely scheme data

Employers and payroll providers

As a default all our employers are required to use the i-Connect portal to submit information. i-Connect automates a number of procedures, which reduces the administration time for both us and the employer. Information is uploaded monthly. It is widely recognised that regular transmission of data dramatically improves data quality which is why we have invested in this tool. i-Connect also includes a number of automated checks on the data provided before it is uploaded to the administration system.

Any employers not submitting data via i-Connect, once it is made available to them, may risk compromising data quality. As referred to previously use of this system is therefore compulsory to all employers and any employers who do not engage with this may be charged administration costs. We monitor the submission of data via i-Connect on a regular basis to ensure all employers are submitting their data in this 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 these requirements.

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. Further information on these controls can be found in the table below.

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 South Yorkshire Pension Fund 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 Fund. 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 Fund, of the death. We download notifications from the TUO service on a daily basis in order 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 monthly 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 appoint a specialist external agency to carry out triennial checks to help us identify when overseas pensioners are no longer entitled to receive benefits.

Monitoring and reviewing data: data cleansing activities

This section outlines our internal data cleansing processes relating to monitoring and reviewing scheme data to ensure it is as accurate, up to date and as complete as possible. We keep records of these activities undertaken including their findings.

We monitor the quality and timeliness of our data in the following ways:

Activity / Category of data	Action	Timescale
Year-end data cleansing (part of Annual Benefit Statement preparation)	Reports are produced to undertake a comparison of contributions received by employers against the CARE pay at year-end for active members, helping to identify errors, including those relating to Assumed Pensionable Pay (APP). In addition, "Error" and "Warning" reports are run and responded to accordingly.	Annually: April to August. However, we are working towards producing these reports on a monthly basis
Pensioner payroll reports	A check is carried out between the amount of pension recorded on the pensioner payroll and the amount held on the pensions administration system.	Monthly
i-Connect data submissions review	Automated checks are made on the data received via i-Connect and any issues or discrepancies are queried with the employer/payroll provider.	Monthly
Reviewing timeliness of joiners, leavers and retirements as part of employer escalation process	Using our KPI model/employer escalation model any trends on late reporting are identified based on a RAG rating and relevant	Monthly

	employers are contacted to agree an improvement plan.	
TPR data scoring	We use the pensions administration software data quality dashboard to assess TPR's two data quality measures - common and scheme specific data. We obtain the scores for each measure on a monthly basis so we can continually work on improving the scores. We report these scores to TPR on an annual basis.	Monthly
Contribution reconciliation	We check employee and employer contributions made by employers against the data we hold on the pensions administration system and investigate any discrepancies.	Monthly
Employer engagement and training	We have a wealth of materials and tools to support our employers in their responsibilities including the accurate and timely submission of data (these materials are outlined in our Pensions Administration Strategy).	Ongoing
Member data validation	We carry out checks on the data provided by members. For example, we check a member's date of birth and date of marriage (if applicable) held on the pensions administration system against their birth/marriage certificate before paying benefits. Our controls relating to other member data validation checks are outlined in our Anti-fraud and Corruption Strategy.	Ongoing

Pensions increase programme	We run the pension increase process in the Test system and error reports are run and issues addressed, before the routine is run in the Live system. The pension increases are run in both the pensioner payroll and pensions administration systems and a comparison made and any discrepancies resolved and adjusted on the pensioner payroll system if required.	Annually
Benefit calculation checks	All benefit calculations are carried out and checked by appropriately qualified staff. This control is enforced using a “skill set-up” on the pensions administration system. This only permits certain qualified staff to check certain calculations and prevents officers from checking a case they have processed.	Daily
Housekeeping reports	Diary reports are set up to ensure that certain date-dependent processes are carried out. Examples include setting up reminders to convert short term pensions to long term pension, checking continued eligibility for/ceasing children’s pensions, age 75+ members, writing to deferred members approaching State Pension Age (SPA), writing to frozen refund members.	Monthly

Member self-checking	We encourage members to review the data provided on communications sent to them and that held on the member self-service portal and inform us of any discrepancies.	Ongoing
KPI monitoring	We are only able to meet our 'overall' KPI measures where we are issued with timely and accurate data by employers. Similarly, we are only able to achieve our internal and legal measures where we already hold accurate data. Therefore, achieving consistent high performance against our KPI measures indicates good quality data.	Monthly
Insights data cleansing dashboard	We use the pension software additional reporting module Insights to monitor the presence, accuracy and format of data items. Insights is also used to support us with our data cleansing in relation to large scale projects such as pensions dashboards. This includes checking for completeness, consistency and format of data: • Complete: there is data in all expected fields • Consistent: for example, date joined is before date left • Format: for example, dates, NI number prefix as expected	Weekly/monthly

Financial checks: including balancing of money against the ledger	We review all payments coming in and out of the Fund on a regular basis and assure they are assigned to the correct cost centre. This includes monthly monitoring and appropriate ledger coding of all income including monies initially coded as miscellaneous on receipt.	Ongoing
---	---	---------

Measuring the Fund against the Policy objectives

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

Objective	Measurement
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	Common and scheme specific data scores of 100%. Common and scheme specific data scores do not decrease year on year. Key Performance Indicators achieved in 90% of cases* (100% for legal requirements). Data issues are not a significant or moderate cause of delays, inaccuracy, or mistaken identity in pensions administration. All data is available in time for Annual Benefit Statements to be issued by the statutory deadline.
To ensure accurate member and transaction records are maintained to support the aims of ensuring employer liabilities are correctly calculated	No assumptions need to be made by the Scheme Actuary based on missing or inaccurate data. No errors are identified in relation to employer liabilities.
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	100% of employers use the secure employer portal to provide monthly data returns. 100% of data is exchanged with third parties using secure, agreed methods. There are no data breaches or cyber incidents.
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	There are no data breaches or cyber incidents Evidence compliance with data monitoring and improvement/record keeping modules in The Pensions Regulator's Code Common and scheme specific data scores of 100% Common and scheme specific data scores do not decrease year on year Key Performance Indicators achieved in 100% of cases for legal requirements

To ensure the roles and responsibilities between the Fund, employers and other stakeholders in relation to data quality are clear and understood	The Pensions Administration Strategy sets out roles and responsibilities Employer escalation procedure in place and when used results in improvement in the timeliness and accuracy of data submitted Annual satisfaction surveys with employers achieving 90% of score in relation to questions about understanding their responsibilities.
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	Data Improvement Plan in place, which is regularly updated evidencing data issues identified, resolved quickly and preventative actions put in place
To ensure data management processes are clearly documented and regularly reviewed.	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.

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. We use our software provider's 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.

Key risks

The key risks to the delivery of this Policy are outlined below. The Pensions Administration Manager (or the Pensions Operations Manager⁶ after that post has been appointed) and other officers will work with the Pensions Advisory Panel, Pension Fund Committee and Pension Board in monitoring these and other key risks and consider how to respond to them.

⁶ All references to the Pensions Administration Manager in this document should be read as Pensions Operations Manager once that position is appointed to.

- Lack or reduction of skilled resources at the Fund, employers or payroll providers could lead to a lack of focus on data quality.
- Significant increase in the number of employing bodies causes strain on employer compliance and liaison.
- Significant external factors, such as national change, impacting data requirements and security of data already held (e.g. the McCloud data collection exercise).
- Employer's failure to provide accurate and timely information or in the correct format resulting in incomplete and inaccurate records which could contribute to delays and inaccurate member benefit entitlements.
- Failure to maintain records adequately, resulting in inaccurate data resulting in inaccurate member benefit entitlements.
- Use of external printers/distributors resulting in data mismatch errors.
- Failure to maintain employer contact database leading to information being sent to incorrect person.
- Cyber incident leading to loss, compromise, or theft of data.

Reporting

We will include an overview of our performance against the objectives in this Policy to Pension Fund Committee and Pension Board on an annual basis (noting there is some overlap of these measures with our Pensions Administration Strategy which are ongoingly reported to Pension Fund Committee and Pension Board). Further data quality measures such as our common and scheme specific data scores are reported on within our Annual Report and Accounts and are reported to Pension Board annually at the next meeting following the scores' submission to TPR. In addition, data quality is a standard item on the agenda of all Pension Board meetings.

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).

Approval, review and consultation

This Policy was approved by the Pension Fund Committee on 19th March 2025. It will be formally reviewed and updated at least every three years or sooner if the data quality management arrangements or other matters included within it merit reconsideration, including if there are any changes to the LGPS or other relevant Regulations or Guidance which need to be taken into account.

In preparing and updating this Policy, other than in relation to minor changes, we have consulted with the relevant employers, the scheme member and employer representatives on the Clwyd Pension Board, and other persons considered appropriate.

Further Information

If you require further information about anything in or related to this Data Quality Policy, please contact:

Karen Williams, Pensions Administration Manager, Flintshire County Council

E-mail: Karen.Williams@flintshire.gov.uk

Telephone: 01352 702963

Appendix A: Data controllers

In order to comply with the Data Protection Act 2018, we and the Employer will separately inform members of the respective purposes for which they will each process members' personal data and provide all required information to ensure that the members understand how their personal data will be processed in each case by us or the Employer (as applicable). The Employer's privacy notice to members will inform them that their personal data will be provided to us and a copy of that notice will be provided to us on request.

The Employer undertakes to notify us as soon as practicable if an error is discovered in the members' personal data of which it is a data controller and which has been provided to us, to ensure that we are then able to correct our own records.

If either we or the Employer appoints professional advisers, third party administrators or another entity which provides other services involving the transfer of members' personal data, those third parties will be data processors or data controllers in their own right. We or the Employer (as applicable) will comply with our or its own obligations in accordance with Data Protection Law (in particular, by ensuring that any entity to which we or it transfers members' personal data also complies with Data Protection Law) and shall ensure that nothing in the terms of engagement between us or the Employer (as applicable) and such third party would contradict Data Protection Law.

We confirm that we understand our obligations under Data Protection Law in the event of any personal data breach, unauthorised or unlawful processing of, loss or destruction of or damage to any of the members' personal data, including (where necessary) an obligation to notify the Information Commissioner's Office and/or the member(s).

Appendix B: Personal Data Retention Policy

Introduction

As data controllers, we are required by data protection legislation to comply with the principles of data minimisation and storage limitation. Personal data we process:

- must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed; and
- must not be kept in a form which permits identification of a data subject for longer than is necessary for the purposes for which the personal data is processed.

We are obliged to retain certain records (whether in hard copy or electronic form) for various periods of time because:

- we have a statutory obligation to do so; and/or
- the information contained in those records may be necessary for the future (for example, questions may arise about the calculation of benefits paid in the past, and data that may be relevant to a possible legal claim needs to be kept until the period within which that claim could be brought has expired).

This policy document sets out the measures we use to comply with the principles of data minimisation and storage limitation in relation to personal data that we hold.

Types of personal data we hold

We hold and process the following types of personal data in relation to Members of the Fund:

- Contact details, including name, address, telephone numbers and email address
- Identifying details, including date of birth, national insurance number and employee and membership numbers
- Information that is used to calculate and assess eligibility for benefits, for example, length of service or membership and salary information
- Financial information relevant to the calculation or payment of benefits, for example, bank account and tax details
- Information about the Member's family, dependents or personal circumstances, for example, marital status and information relevant to the distribution and allocation of benefits payable on death
- Information about the Member's health, for example, to assess eligibility for benefits payable on ill health, or where the Member's health is relevant to a claim for benefits following the death of a Member of the Fund
- Information about a criminal conviction if this has resulted in the Member owing money to the Member's employer or the Fund and the employer or Fund may be reimbursed from the Member's benefits.

We hold and process the following types of personal data in relation to Beneficiaries of the Fund:

- Contact details, including name, address, telephone numbers and email address
- Identifying details, including date of birth, national insurance number
- Information about the Beneficiary's family, dependents or personal circumstances, for example, marital status and information relevant to the distribution and allocation of any balance of benefits payable on the related Beneficiary's death
- Information that is used to calculate and assess eligibility for benefits, for example, length of service or membership and salary information (including relating to the related Member)
- Financial information relevant to the calculation or payment of benefits, for example, bank account and tax details.

Retention periods for personal data

In compiling our policy on the retention of personal data, we have taken into account the guidelines on the retention of personal data as set out by / in:

- Information and Records Management Society;
- The National Archives;
- HMRC compliance handbook manual CH15400;
- Lord Chancellor's Code of Practice on the Management of Records issued under Section 46 of the Freedom of Information Act 2000;
- Information Commissioner's Office's guidance on storage retention; and
- The Pensions Regulator's code of practice 14 for public service pension schemes.

Data protection legislation requires that we retain personal data for no longer than is necessary in order to fulfil the purpose(s) for which it is processed. Given the long term nature of pensions, we need to ensure that personal data is retained to:

- comply with our legal and regulatory obligations regarding the payment of pensions from the Fund; and
- deal with any questions or complaints that we may receive about our administration of the Fund

We will retain personal data for **the greater of:**

- such period as the Member (or any beneficiary who receives benefits after the Member's death) are entitled to benefits from the Fund and for a period of 15 years after those benefits stop being paid;
- 100 years from the Member's date of birth;
- 100 years from the date of birth of any beneficiary who received benefits from the Fund after the Member's death

During any period when we retain personal data, we will keep that personal data up to date and take all reasonable steps to ensure that inaccurate data is either erased or rectified without delay. We will periodically review the personal data that we retain and consider whether it is still required; any personal data that we no longer require will be destroyed.

Member's and Beneficiary's rights

Beneficiaries form a wider category of people who receive benefits from the Fund, for example the active/deferred/pensioner Member's spouse / child(ren) / dependents who may receive benefits from the Fund following a member's death. Members of the Fund and Beneficiaries have a right to access and obtain a copy of the personal data that we hold about them and to ask us to correct personal data if there are any errors or it is out of date or incomplete.

In certain circumstances a Member / Beneficiary has the right to:

- object to the processing of their personal data;
- require us to restrict the processing of their personal data until any errors are corrected;
- require us to transfer their personal data; or
- require us to erase their personal data.

If the exercise of the Member's/ Beneficiary's rights would prevent us from paying or continuing to pay a pension from the Fund, we will consider retaining a minimised version of that Member's / Beneficiary's personal data in order to fulfil our legal and regulatory obligations.

Participating Employers

This policy applies to Flintshire County Council in its capacity as the administering authority of the Fund. We have produced separate guidance for other participating employers in the Fund about our expectations for the retention by them of personal data we may require to administer the Fund. That guidance includes a suggested data retention policy that employers can each adopt in relation to their participation in the Fund.



clwydpensionfund.org.uk

Tŷ Dewi Sant, St. Davids Park, Ewloe, Flintshire, CH5 3FF

Please note that Flintshire County Council is the Administering Authority of the Clwyd Pension Fund and we use your personal data in accordance with Data Protection legislation to provide you with a pension administration service. For more information about how we use your data, who we share it with and what rights you have in relation to your data, please visit the Privacy Notice on our website.