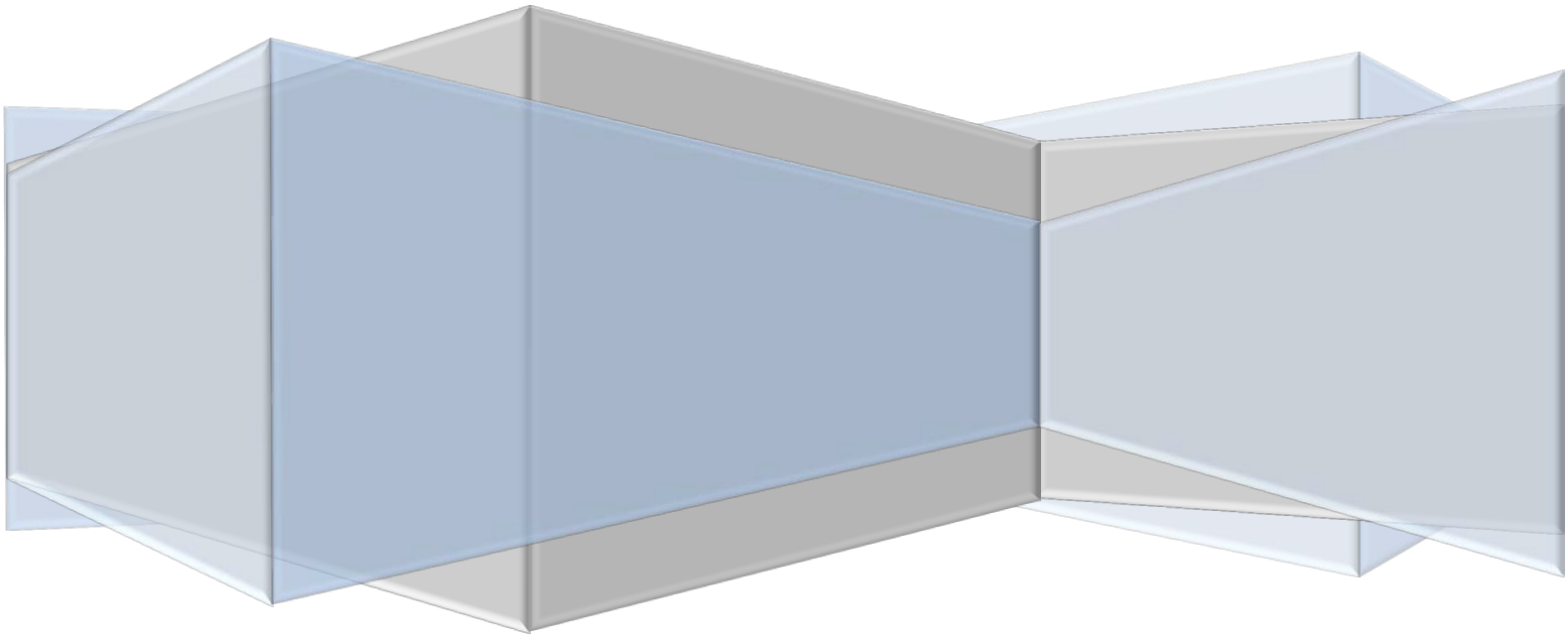
Data Protection Policy

Draft for Local Pension Board Review



This document has been presented, considered and approved by Pension Committee on xx xxx xxxx, following consultation with the Local Pension Board.

Contents

1. Introduction

The Merseyside Pension Fund (the Fund) is one of the largest Local Government Pension Schemes in the UK and manages the pension records of over 135,000 members. The Fund is not a legal entity in its own right, but sits as a function of Wirral Metropolitan Borough Council (the Council) who hold the capacity of Administering Authority.

The Council, and therefore the Fund, are classed as a Data Controller under the Data Protection Act 2018 (the Act) as it collects, stores and controls how personal information relating to its members is managed.

The Act is the UK implementation of the General Data Protection Regulations (GDPR) which came into force on 25 May 2018.

Consequently, it is required to hold, manage and process any personal data fairly, lawfully and in accordance with all Data Protection legislation, including

2. Purpose

The purpose of this policy is to define the Fund's responsibilities under the Act, providing assurance to our members that their data is managed in compliance with the statutory obligations placed upon the Fund.

This policy is designed to give members an overview of how the Fund complies with the Act in our working practices and to provide an overview to Fund officers of how the Act should be applied to inform their decisions and day-to-day work by providing a legal background to the processing of personal data.

3. Scope

This policy applies to all employees, officers, Pension Committee members, Pension Board members, contractors and partner agencies who:

- Process personal data as part of their role or on behalf of the Fund (including contracted service providers);
- Have access to the Fund's administration system(s) for purposes of maintenance and/or service provision in line with a contracted duty;
- Have access to buildings where personal data is stored.

4. Review

This policy will be reviewed on an annual basis by the Fund, and in line with the Council's adopted programme of formal review.

5. Definitions

a) **Personal Data –** any information relating to an identified or identifiable natural person which includes members, next of kin and any other associated individual.

b) **Sensitive Personal Data –** data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

c) **Processing Personal Data –** is essentially any action involving personal data, this can include storing, sharing, creating, altering, organising or deleting. It is not limited to these examples and applies to both physical and electronically held data.

d) **Data Subject –** is an individual who is the subject of personal data.

e) **Data Controller –** is a person or organisation who decides the purposes for processing personal data. The Fund is a data controller.

f) **Data Processor –** is a person or organisation who processes personal data on behalf of the controller (other than a person who is an employee of the controller).

g) **Information Security Officer** (ISO) – Is the person within the organisation that is responsible for the development and implementation of information security policies to protect the organisation's information assets. Information Security relates to more than just personal data. The ISO for the Fund is a designated officer within the Digital/IT Services section of Wirral Metropolitan Borough Council.

h) **Data Protection Officer** (DPO) – Is the designated person within an organisation that has responsibility for ensuring 'legal' compliance with the Data Protection Act, which relates only to personal data.

6. Categories of Data

a) **Personal data –** This relates to data about an individual which is not classified as a special category of personal data and can include information relating to contracts of employment and salary.

b) **Special categories of personal data** – Sensitive personal data as defined in the Act may relate to members where relevant to the Fund's assessment on entitlement of benefits in-line with the LGPS regulations e.g. medical history and occupational health assessment

c) **Pensions data –** this may relate to information relating to a member's previous pension benefits accrued either with this Fund or another fund which will need to be considered when assessing pension entitlement.

d) **Employer data** – information relating to the Fund's employers for who the Fund will hold individual officer contact details for the purposes of communication and administration of the LGPS.

7. Overseas Data Transfer

The Fund does have a number of overseas members who reside in countries other than the UK, and also outside the European Union. Other than the necessary data required to make pension payments to overseas members (name and bank account), the Fund does not systematically transfer personal data relating to overseas members to any organisation outside of the jurisdiction of the Act and/or the General Data Protection Regulations.

8. The Six Principles of Data Protection

The Act sets out the main responsibilities for organisations in regard Data Protection, and requires organisations to show **how** they comply with its six principles.

Data Protection Principle	Fund Position
1. Processed lawfully, fairly and in a transparent manner in relation to individuals	The Fund provides pension benefits to over 135,000 members who are automatically enrolled into the Fund on commencing their employment with an eligible employer. Members are provided with joiner information by their employer which notifies them of their enrolment into pension saving, followed by joiner information from the Fund confirming their membership. The new joiner information pack contains references to the Privacy Notice, confirming how their information is used, and with whom it is shared.
2. 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.	The Fund collects information from the member's employer regarding that member's employment (salary, contact information, and past service details). Information is also obtained from the member direct about any other pension benefits they may hold. This information is required by statute in order to process a member's pension account.
3. Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.	The Fund may hold information which is not immediately relevant (nomination details of third parties for example) however, due to the nature of the pension provision, the benefits may become payable at any given date and it has been determined that the information would be relevant and required at the point the pension benefits are payable. The Fund therefore has assessed that this information is relevant and specific to meeting its duties as an LGPS fund.

Data Protection Principle	Fund Position
4. Personal data undergoing processing must be accurate and, where necessary, kept up to date.	Members have access to the MyPension, self-service platform where they can securely log on and review their basic personal details and review their pension entitlements as either an Annual Benefit Statement or a Payslip if the member is already in receipt of benefits. The Fund performs periodic data reconciliation exercises with employers in addition to the annual contribution returns exercise. This is a key exercise in maintaining the accuracy of contributing member information. In relation to the Fund's deferred members, who have moved away and lost contact with the Fund, our administration responsibilities require working with approved third party partners to trace members based on their previous address. The Fund has a published Privacy Notice detailing member's rights in regard their data.
5. Personal data must be kept for no longer than is necessary for the purpose for which it is processed.	The Fund, in providing statutory duties under the regulations has determined that it cannot permanently delete a member's record; this limitation is published within the Privacy Notice. Basic member details are required to be retained to enable the Fund to comply with statutory and legal obligations such as actuarial assessment, fraud prevention and Guaranteed Minimum Pension (GMP) reconciliation.
6. Processed in a manner that includes taking appropriate security measures as regards risks that arise from processing personal data.	The Fund's IT environment is provided by the Council and areas such as Cyber Security fall within the remit of the Digital section. The Fund's Operations & Information Governance Manager is the link officer with the corporate functions of the Council, in regards data protection, data security and information policy development. When contracting third parties, the Fund requires all service providers to be compliant with the Act and the duties defined within the GDPR. This is documented within the contractual arrangements, and all existing suppliers have provided acceptable addendums to their contracts of services.

9. Legal Basis for Processing

The legal basis for our processing of personal data will generally be one or more of the following:

- We need to process the personal data to satisfy our legal obligations as the Administering Authority of the Fund; and/or
- We need to process the personal data to carry out a task in the public interest or in the exercise of official authority in our capacity as a public body; and/or
- We need to process the personal data for the legitimate interests of administering and managing the Fund and liabilities under it, calculating, securing and paying benefits and performing our obligations and exercising any rights, duties and discretions the Administering Authority has in relation to the Fund; and/or
- Because we need to process the personal data to meet our contractual obligations to the member in relation to the Fund. For example, under an agreement that they pay additional voluntary contributions to the Fund.

10. Process for Data Subject Requests

Subject Access Requests

A data subject has the right to access and obtain a copy of the personal data that an organisation holds. In the first instance, members are invited to request a Subject Access Request (SAR) of the Fund's Data Protection Officer.

The Fund will act upon the SAR without undue delay and at the latest within **one month** of receipt. The Fund will calculate the time limit from the day after it receives the request (whether the day after is a working day or not) until the corresponding calendar date in the next month.

If required, the Fund may ask the member for more information to clarify their identity or to clarify the details of their request. The Fund, may, on occasion, action an extension to the one month timeframe and reserves the right to charge a reasonable fee for unfounded or excessive requests by the data subject, as the Act allows.

Depending upon the scope of the member's request, liaison with the Council's Data Protection Officer may be required in order to fully comply with the request.

The Act does not prevent an individual making a SAR via a third party e.g. a solicitor. In these cases, the Fund needs to be satisfied that the third party making the request is entitled to act on behalf of the individual; however it will be the third party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request, or it might be a more general power of attorney.

Complaints or Corrective Action

Where an individual data subject has a question or complaint regarding how their rights under the Act are upheld, they are encouraged to make contact in writing (or email) to the Fund's Data Protection Officer in the first instance.

Data subjects who consider that data is inaccurate or out-of-date are encouraged to use the online MyPension system to check the data held by the Fund and to submit a request for correction. Where that is not possible, they may also request, in writing, that the information be corrected or erased.

They will receive a written response indicating whether or not the Fund agrees and if so, the action to be taken. In the event that the Fund disagrees (eg. the data is held for a legal purpose), the data subject may request their objection be recorded with the relevant record.

Data subjects may ask the Fund for an explanation of any decision likely to significantly affect them which has been, or may be, taken solely by wholly automated means, this will apply most specifically in the electronic calculation of pension benefits using the Fund's administration system. The Fund will consider a request and consider reviewing a decision which has been taken, or, consider taking a new decision on a different basis, in circumstances where either course of action is appropriate and timely, unless the automated decision qualifies as an exempt decision.

If a data subject remains dissatisfied with a response received, they may ask for the matter to be dealt with under the Fund's Internal Disputes Resolution Procedure (IDRP)

Ultimately if a data subject continues to be dissatisfied, she/he has the right to ask the Information Commissioner's Office (ICO) to carry out an assessment of their case and/or pursue a legal remedy.

11. Responsibilities

Wirral Council as the administering authority provide the computer network infrastructure for the Fund and the supporting procedures and guidance for staff on Information Governance issues; including Data Protection.

The Council also defines a corporate approach to data protection and information governance, this includes the provision of suitable periodic training to be undertaken by Fund officers as appropriate.

The Fund's Operations & Information Governance Manager is a member of the Council's Information Governance Delivery Group (IGDG) to ensure knowledge, compliance and to make a contribution towards the development of a technical and policy framework around Data and Information.

Fund Data Protection Officer

This role is undertaken by the Fund's Operations & Information Governance Manager, who has liaison and compliance responsibilities with the Data Protection Officer of Wirral Metropolitan Borough Council.

Breaches of Policy & Security Incidents

Breaches of this policy and/or security incidents can be defined as events which could have, or have resulted in, loss or damage to an individual's personal data which is in breach of the Fund's security procedures, policies and the Data Protection Act.

The Act imposes a duty on all organisations to report certain types of data breaches to the relevant supervisory authority within 72 hours of becoming aware, and in some cases to the individuals affected.

All employees, officers, Pension Committee members, Pension Board members, contractors and partner agencies have a responsibility to report security incidents and breaches of this policy as quickly as possible to the Fund's Data Protection Officer. This obligation also extends to any external organisation contracted to support or access the Information Systems of the Fund.

In the case of third party vendors, consultants or contractor's non-compliance could result in the immediate removal of access to the system. If damage or compromise of the Fund's ICT systems or network results from the non-compliance, the Fund may consider legal action against the third party.

The Fund will take appropriate measures to remedy any breach of the policy through the relevant frameworks in place. In the case of an individual then the matter may be dealt with under the disciplinary process.

Any incidents of data breach or near miss should be reported to the Fund's Data Protection Officer.

12. Supporting Documentation

Privacy Notice & Fair Processing Notice

The Fund publishes these key documents on the main members' website at:

http://mpfund.uk/yourdata

Wirral Council Data Protection Information

As the Administering Authority, the Council provides a supporting policy framework in regard Data Protection and Information Governance. More information can be obtained from the Council website at:

https://www.wirral.gov.uk/about-council/freedom-information-and-data-protection/data-protection-act

Approved by: Pensions Committee xx xxx xxxx

Merseyside Pension Fund
Castle Chambers, 43 Castle Street
Liverpool, L2 9SH

Telephone: 0151 242 1390
Fax: 0151 236 3520

Web: mpfmembers.org.uk
mpfemployers.org.uk

Email: mpfadmin@wirral.gov.uk