DATA PROTECTION POLICY
JANUARY 2021

West Midlands Pension Fund

CONTENTS

Version:	3.0
Author:	Rachel Howe, Head of Governance and Corporate Services
Date:	January 2021
Review Date:	January 2023

INTRODUCTION

The West Midlands Pension Fund (the Fund) is one of the largest Local Government Pension Schemes (LGPS) in the UK and manages the pension records of over 330,000 members. The Fund is not a legal entity in its own right, it sits as a function of the City of Wolverhampton 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 Laws (DPL) as it collects, stores and controls how personal information relating to its members is managed. Consequently, it is required to hold, manage and process any personal data fairly, lawfully and in accordance with all applicable DPL.

PURPOSE

The purpose of this policy is to define the Fund's responsibilities under DPL, 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 DPL in our working practices. This policy also provides an overview to Fund officers of how DPL should be applied to inform their decisions and day to day work, by providing the legal basis for the Fund's processing of personal data.

SCOPE

This policy applies to all Fund officers, Pensions Committee and Local Pensions Board members, contractors and third party 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 member software system for purposes of maintenance and or/ service provision in line with a contracted duty
- Have access to buildings where personal data is stored

POLICY STATEMENT

This policy forms part of the Fund's Data Management Framework and should be read in conjunction with the following:

- Freedom of Information Policy
- Data Quality Policy
- Cyber Security Strategy
- Information Incident Management Policy

DEFINITIONS[1]

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, 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, which 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) **Business Data** – is any information required when carrying out business activities. The non-exhaustive list includes employee information, investment advice, operating procedures, intellectual property, transactions, policies and valuations.

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

f) **Data Controller** – is a person or organisation who decides the purposes for processing personal data and business data. The Fund is a data 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 West Midlands Pension Fund is the Head of ICT at the City of Wolverhampton Council.

h) **Data Protection Officer (DPO)** – Is the designated person within an organisation that has responsibility for ensuring 'legal' compliance with DPL, which relates only to personal data. The DPO for the West Midlands Pension Fund is the Head of Governance and Corporate Services.

CATEGORIES OF INDIVIDUALS

The Fund, in providing pension benefits to its members, categorises its membership into three distinct profiles, active, deferred and pensioner members. These are expanded on below:

Active Members
This relates to members of the Fund who are presently employed with a Fund Employer and are contributing to their pension benefits. The personal data held by the Fund is jointly controlled by the Fund and the Employer.

Deferred Members - Employed
This relates to members of the Fund who are presently employed by a Fund Employer and who in the past have contributed to their pension benefits but have chosen not to currently contribute to their pension benefits. The personal data held by the Fund is jointly controlled by the Fund and the Employer.

[1] The DPA contributes to and translates the definition of a data controller in section 6 of the Act.

Deferred Members – No Longer Employed
This relates to members of the Fund who are no longer employed by a Fund Employer, but whose pension benefits remain with the Fund. The Fund distinguishes these from the above category of members as the Fund is a single data controller. This is due to members no longer having a contractual relationship with the Employer and the Employer no longer having access to their personal data.

Pensioner Members
These are members who are in receipt of their pension benefits. The Fund is the single data controller for these members.

Beneficiary Pensioners
These are members who have inherited pension rights from their spouse, family member, or another individual. The Fund is the single data controller for these members.

Other Third-Party Data
The Fund may hold information relating to members' next of kin, for example on a nomination form. The Fund is a data controller for these persons and holds the information under section 8 (c) of the DPA as the holding of the information is necessary for the purpose of making a determination in connection with eligibility for pension benefits.

SPECIAL CATEGORIES OF DATA

The Fund has identified that it holds data in the following distinct categories:

Special Categories of Data
This relates to sensitive personal information as defined in the DPL and may relate to members of the Fund or other third-party data. This may also include medical history where relevant to the Fund's assessment of entitlement of benefits in line with the regulations.

Personal Data
This relates to data about an individual which does not belong to a special category of data. This can also include information relating to contracts of employment, pension contributions and salary.

Pensions Data
This may relate to information regarding a member's previous pension benefits, accrued either with this Fund or another fund which will need to be considered when assessing entitlement.

Employer (Business) Data
This is information relating to the Fund's employers for who the Fund may hold individual officer contact details.

OVERSEAS DATA TRANSFER

The Fund does have a number of overseas members who reside in countries other than the UK. The majority of these are in European countries, USA or Australia. The Fund does not transfer data relating to overseas members to anyone other than the individual member or a third party for which we have received a Fund-specific authority form.

THE SIX PRINCIPLES OF DATA PROTECTION

The data protection principles set out the main responsibilities for organisations with the most significant addition being the accountability principle which requires organisations to show how they comply with the following principles.

The below principles are drawn from Data Protection Laws and the Fund has an obligation to outline how the requirements of these laws are complied with.

The table below sets out how the Fund adheres to these principles.

Principles	Fund Position
1) Processed lawfully, fairly and in a transparent manner in relation to individuals.	The Fund provides pension benefits to over 330,000 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 enrollment in the Fund and also receive a new joiner's information pack from the Fund confirming their membership. The new joiner's information pack contains a standard Data Protection paragraph, which directs members to the Privacy Notice confirming how their information is used, and with whom it is shared. The member's rights are also outlined in the Privacy Notice and provide details on how a member can ask questions or request information relating to these rights.
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 a member's employer regarding that member's employment (salary, contact information, and past service details). Information is also obtained directly from the member in regard to other pension benefits they hold. This information is required by statute in order to manage and administer a member's pension account. The Fund reviews the information received from employers, ensuring it is relevant to the performance of its duty as a local government pension provider. This ensures that the information it holds is specific and relevant for the purposes it was collected. 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. This information would be relevant and required at the point the pension benefits are payable.

Principles	Fund Position
3) Adequate, relevant and limited to what is necessary in relation to the purposes for which it permits identification of data subjects for no longer than is necessary for the purposes for which the personal processed.	The Fund reviews the information received from employers, ensuring it is relevant to the performance of its duty as a local government pension provider. This ensures that the information it holds is specific and relevant for the purposes it was collected. 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. This information would be relevant and required at the point the pension benefits are payable.
4) 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.	The Fund's Pensions Portal platform is an additional tool for ensuring the information held about members is accurate, enabling members to self-serve and rectify the data the Fund holds about them. In line with its statutory requirement the Fund implements its Data Management Strategy to ensure accurate and complete pensions data. This requires employers to submit a monthly data file about their employees who are members of the Fund, enabling rectification of the information held by the Fund ensuring its current and ongoing accuracy. In relation to the Fund's deferred members, the Fund continues to engage this group to encourage them to sign up to the Pensions Portal and take responsibility for their own personal data held by the Fund. In addition, The Fund has implemented a rolling member tracing programme which seeks to locate deferred members with a retirement date in the forthcoming years. This ensures the information held is accurate at the point of retirement so that the Fund can comply with its statutory duty to pay pension benefits when they fall due. The Fund has published a Privacy Notice which outlines a member's rights to request rectification of their data and how to make this request.
5) 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;	The Fund, in providing statutory duties under the regulations has determined that it cannot permanently delete a member's record, regardless of their membership status.

Principles	Fund Position
personal data may be stored for longer periods insofar 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 in order to safeguard the rights and freedoms of individuals.	As a minimum, the basic member details are required to be retained to enable the Fund to comply with statutory and legal obligations such as fraud prevention and GMP reconciliation.
6) 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.	The Fund has adopted a Cyber Security Strategy which outlines how the Fund protects members' data from incidents of Cyber Crime, outlining the Fund's control mechanisms for its pension administration software system. When contracting with third parties (as outlined in the Privacy Notice) who will have access to Fund member data or information, the Fund requires these third parties to enter into a Data Sharing Agreement (DSA). This DSA sets out the Fund's expectations of the third party in line with data protection legislation. As part of the Fund's annual assurance programme, third parties whose contract is longer than twelve months are required to submit annual assurance questionnaires confirming continued compliance. When engaging with members, the Fund has implemented security identity check processes which require members to pass three identification questions when contacting the Fund.

NOTABLE SECTIONS UNDER THE DPL

Section 8 Lawfulness of Processing Conditions
Under DPL, organisations need to identify a lawful basis on which they can process an individual's data. These are referred to as the "conditions for processing".

An organisation will be required to ensure it meets the conditions for processing and will need to explain to individuals whose data it holds, how it meets those conditions and what the individuals' rights are to ensure their data is managed appropriately.

The Fund's lawfulness for holding and managing member's data falls under Section 8(c)[2] in that we are providing a statutory pension to our members.

[2] Data Protection Act s.8 laid out in further detail in Schedule 1 of the Act.

The table below sets out the lawful basis from the DPL for processing personal data, and how the Fund manages members' data in line with this to provide assurance to members of the Fund's management of their data.

Condition	Fund Position
Consent of the data subject.	The Fund, as a Local Government Pension Scheme Fund provides statutory pension benefits to all its members, it therefore has a lawful purpose for holding personal data. Active members are automatically enrolled into the Fund through their employment contract and have the option to opt-out once in employment. Deferred members are statutorily entitled to receive their pension benefits at their normal pension age. Pensioner members are statutorily entitled to receive their pension benefits and any inflationary increase.
Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract.	As a statutory scheme, there is no formal contract with individual members, however the statutory duty to provide pension benefits to eligible employees is interpreted by the Fund as a binding agreement.
Processing is necessary for compliance with a legal obligation	The Fund, as a Local Government Pension Scheme Fund provides statutory pension benefits to all its members and may rely on this condition when processing member data.
Processing is necessary to protect the vital interests of a data subject or another person.	As a pension provider, the Fund may hold details of a member's next of kin/family member/associates, whose details are held for the purpose of beneficiary pension payments. The information we hold on these third parties will be provided by the member. The Fund considers that it holds this data in line with this condition as it may be required to pay pension benefits to those individuals in any point in the future.
Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.	The Fund, as a Local Government Pension Scheme Fund provides statutory pension benefits to all its members and may rely on this condition when processing member data.
Necessary for the purposes of legitimate interests pursued by the data controller.	While at first, this condition may appear to be relevant to local authorities in the performance of their duties, guidance from the Information Commissioner (ICO) states that authorities cannot rely on this condition when processing personal data. As such the Fund may rely on the other conditions for processing members' data as outlined above.

Section 10 Special Conditions for Sensitive Personal Data
In addition to the above conditions, where an organisation processes sensitive personal data, it must also comply with further DPL regulation[3].

The table below sets out how the Fund complies with this Article.

Condition	Fund Position
Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State Law.	The Fund, as a Local Government Pension Scheme Fund provides statutory pension benefits to all its members. Active members are automatically enrolled into the Fund through their employment contract and have the option to opt-out once in employment. Deferred members are statutorily entitled to receive their pension benefits at their normal pension age. Pensioner members are statutorily entitled to receive their pension benefits and any inflationary increase.
Processing is necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement.	The Fund, as a Local Government Pension Scheme Fund provides statutory pension benefits to all its members who become eligible through their employment contract. The Fund applies this condition when processing member data.
Processing is necessary to protect the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.	The Fund may have members of the scheme who operate under a Power of Attorney / court order whereby responsibility for their affairs is granted to family members or guardians. The Fund applies this condition when processing the sensitive data of those members and their families.
Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to member or former members.	This condition is not relevant to the work of the Fund.
Processing relates to personal data manifestly made public by the data subject.	This condition is unlikely to be relevant to the work of the Fund.
Processing is necessary for the establishment, exercise or in defense of legal claims or where courts are acting in their judicial capacity.	This condition may apply to the Fund as it strives to prevent fraud or duplicate claims from individuals. The Fund may also be subject to challenge under the Internal Dispute Resolution Procedure (IDRP) and may require the retention of personal data to defend such claims.

[3] Data Protection Act s.10 laid out in further detail in Schedule 1 of the Act.

Condition	Fund Position
Processing is necessary for reasons of substantial public interest on the basis of Union or Member State Law which is proportionate to the aim pursued and which contains appropriate safeguards.	This condition is unlikely to be relevant to the work of the Fund.
Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State Law or a contract with a health professional.	This condition is not relevant to the work of the Fund however, the Fund may receive medical documentation from third parties which may require the retention of personal data. For example, ill health retirement application documents.
Processing is necessary for the reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices.	This condition is not relevant to the work of the Fund.
Processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes.	This condition is not relevant to the work of the Fund.

INDIVIDUALS' RIGHTS

One of the key obligations of organisations who manage, and control individuals' data is to ensure the individual is informed about their rights under Data Protection Laws, which gives them control over how their information is used and by whom[4].

These rights are detailed as follows:

a) The Right to be Informed

This is the right to know how information is used and who it will be shared with. The Fund publishes its Privacy Notice on its website, which outlines what personal information the Fund will hold, who it will share it with and for how long the information will be held.

[4] The DPA now imposes duties on data controllers (see s.44 DPA) which coincide with the right to be informed under the UK GDPR. For example, in s.44 (2) (a) controllers must supply data subjects' information about the legal basis for its processing of data, which has been outlined in this document. Furthermore s.44 (1) (b) the contact details of the Data Protection Officer must be provided. Incidentally the contact email address of the DPO officer is: wmpfdataprotectionofficer@wolverhampton.gov.uk. For further follow up queries.

Should an individual feel that the information supplied in the Privacy Notice is inadequate or that it does not inform them about the how their information is used by the Fund, please contact the Fund's Data Protection Officer for more information at wmpfdataprotectionofficer@wolverhampton.gov.uk

b) The Right of Access

This is an individual's right to obtain

- confirmation that data is being processed[5]
- access to personal data[6]
- access to policies and information held by the Fund about how it uses data[7]

This right enables individuals to verify that the Fund is using data appropriately as well as providing access to obtain copies of information it holds.

Individuals are entitled to see the information held and can request a copy by emailing WMPFSAR@wolverhampton.gov.uk. Copies of the information requested will be provided within one month of receiving a validated request, where the individual member can be identified, with their identification verified through supporting information, however should a request be more complex, the Fund's administering authority, City of Wolverhampton Council may write to an individual or third party, informing them of any potential delay and when the information will be provided[8].

c) The Right to Rectification

Individuals have a right to have information amended or rectified if they believe it is inaccurate or incomplete.

If you believe any information we hold about you to be incorrect, please email pensionfundenquiries@wolverhampton.gov.uk and we will amend the information accordingly.

The West Midlands Pension Fund operates a self-service platform called "Pensions Portal" where members can amend details the Fund holds about them, including name, address, bank details and nominations. Members are encouraged to use this platform to ensure the information the Fund holds about them is accurate and up to date[9]. The Fund's Pensions Portal can be accessed at https://www.wmpfonline.com/pensionsportal.

d) The Right to Erasure/Right to be Forgotten

This right allows individuals to request a company or body to delete any or all information they hold about them. However, the right to erasure does not provide an absolute 'right to be forgotten'. Individuals have a right to have personal data erased and to prevent processing in specific circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed (i.e. otherwise in breach of the DPA)

[5] s.45 (1) (a) of the DPA.
[6] s.45 (1) (b) of the DPA.
[7] s.44 (1) (c) is the provision which instructs the Fund to give access to the information of how it uses subjects' data. s.44 in general instructs the Fund to make its policies available for public viewing.
[8] s.45 (3) and s.54 of the DPA gives guidance on how long the Fund has to reply to requests of access.
[9] s.46 of the DPA is the provision in relation to the Right to Rectification.

- The personal data must be erased in order to comply with a legal obligation[10]

The Fund, in providing statutory duties under LGPS regulations has determined that it cannot permanently delete a member's record. Should a member transfer out of the scheme, the Fund will retain a basic record confirming the member's name, contact, date of birth and national insurance number and any relevant documents determined by the Fund to support future statutory processing. The basic member details and documents are required to be retained to enable the Fund to comply with statutory and legal obligations such as fraud prevention and GMP reconciliation.

e) The Right to Restrict Processing

Individuals have a right to limit how the Fund uses data, including who it shares it with[11].

A request for information to be used for limited purposes will not result in the deletion of the information the Fund holds. Requests to restrict processing will be considered on a case by case basis, with the decision determined by the Fund's Data Protection Officer.

The Fund publishes a Privacy Notice which outlines how it uses data and who it shares it with. Should you wish the Fund to limit how we use your data please email wmpfdataprotectionofficer@wolverhampton.gov.uk with the reasons for your request.

f) The Right to Data Portability

This right enables individuals to obtain copies of the information the Fund holds in a format that is easily transferred to either individuals or another organisation.

This is particularly relevant to members who may choose to transfer out of the Fund to another LGPS Fund or separate pension provider. The Fund will provide the information it holds to a new pension provider in a format that they can use. The transfer of pension benefits would not take place without the consent of the scheme member. In all cases the Fund would retain basic information about a member who has transferred out to prevent fraud and support the Fund's ability to respond to statutory queries (HMRC/GMP).

g) The Right to Object

In addition to the right to limit the use of data, individuals also have a right to object to the use of data for certain actions.

The Fund may share information with third parties, such as consultants or service providers. Under DPL you can object to the Fund sharing your data with these third parties.

Should an individual exercise their right to object, it will not limit the information they receive from the Fund, as it may still be required by law to provide certain information, such as annual benefit statements. Where an individual exercises their right to object, the Fund will take all reasonable steps to ensure requests are complied with, but that it also fulfils any legal obligation it has to provide information or supply services.

h) Children's Data

DPL specifically ensure the protection of children's data, as children may be less aware of the risks and consequences associated with the processing of their personal data.

Any information held by the Fund which relates to the personal data of a child under 13 is held with the consent of the parent or the person with legal parental responsibility.

Children aged 13 – 16 are generally regarded as having the appropriate level of understanding to provide their own consent for the use of their data, provided the Privacy Notice has been written in a way they can understand.

[10] s.47 of the DPA outlines instances and to the nature of the data where deletion of personal data must be done upon request.

[11] Restrict processing is a right conferred from the UK GDPR into the DPA via s.47 (2) to (4).

PROCESSES FOR REQUESTS

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

Data subjects who believe that their data is inaccurate or out of date are encouraged to use the online Pensions Portal to check the data held by the Fund and to attempt to rectify it themselves. Where that is not possible, they may also request, in writing, that the information be corrected or erased. Individuals 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 (e.g. the data is held for a legal purpose), the data subject may request their objection be recorded with the relevant record.

A notice may be served by the data subject objecting to the processing and/or way in which the information is being processed, requesting the Fund to cease doing so on the basis that this may cause substantial unwarranted damage or distress to the data subject. A written response indicating the Fund's intentions will be given within 21 days of receiving the request. This will explain whether or not the Fund intends to comply with the request, including any parts of the request which the Fund considers unjustified.

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 software management system. The Fund will review requests on an individual basis, and consider reviewing a decision, or, consider taking a new decision, 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 Dispute Resolution Procedure (IDRP). Ultimately, if a data subject continues to be dissatisfied, they have the right to ask the Information Commissioner's Office (ICO) to carry out an assessment of their case and/or pursue a legal remedy.

PROCESS FOR REASONS OF LEGAL DUTY

The Fund may receive requests for information from various sources. This can include court orders, or requests under Schedule 2 Part I (para 2) Crime & Taxation or (para 5) Legal Proceedings of the Data Protection Act 2018.

All external agencies, contractors or Service Level Entities (SLEs) that the Fund contracts with must demonstrate the technical and legislative ability to uphold the principles of the Act and the rights of the individual when handling or receiving Fund owned personal data.

The Fund will write, uphold and review Data Sharing Agreements when sharing information with Joint Data Controllers and Service Providers where the exchange of personal data is required. The Fund will ensure that appropriate contracts and Data Sharing Agreements are in place when using third party contractors as data processors. All of the Fund's Data Sharing Agreements are written in line with the ICO's Data Sharing Code of Practice, ICO's guidance on the role of Data Controllers and Data Processors and the Fund's Data Management Framework.

RESPONSIBILITIES

The Head of Governance and Corporate Services in their role as Data Protection Officer is responsible for ensuring compliance with this policy and overall data management and information governance across the Fund.

The Fund will continue to ensure that all employees responsible for handling personal data will receive appropriate training in the use and control of this data. Fund officers responsible for sensitive personal data will also receive training appropriate to their roles.

The Fund continues to implement information incident management procedures to ensure all staff know when and how to report any actual or suspected data breach, and that appropriately trained staff manage these breaches correctly, lawfully and in a timely manner.

All Fund staff must complete the Council's mandatory Protecting Information awareness training and more in-depth training where required.

The Fund will monitor and review its processing activities to ensure these are consistent with the principles and individual rights under DPL.

The Fund will ensure that any new or altered processing identifies and assesses the impact on a data subject's privacy as a result of any processing of their personal data, and that Data Privacy Impact Assessments are completed where appropriate.

The Fund will ensure that any new, altered or existing information assets are recorded and monitored on our Information Asset Register, which as a minimum will be reviewed annually.

BREACHES OF POLICY

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 and policies and DPL.

The DPA (s.67 (1)) 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, Committee and Board members, partner agencies, contractors and service providers have a responsibility to report security incidents and breaches of this policy as quickly as possible through the Fund's Data Incident Reporting Process. 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 a Fund employee, the matter may be dealt with under the disciplinary process.

REVIEW

A review of this policy will take place when appropriate to taking into account new or changed legislation, regulations or business practices. As a minimum this policy will be reviewed biennially by the Fund's Governance team to ensure it remains up to date with Fund processes, procedures and business objectives.

West Midlands Pension Fund
PO Box 3948
Wolverhampton
WV1 1XP