



Staffordshire
Pension Fund
Local Government Pension Scheme

Pension Services

General Data Protection Regulation (GDPR) Policy

Issue Date - 25 May 2018

Review Date - 1 June 2019

Version 1.1



| | |
|--|----|
| Contents | |
| Introduction | 1 |
| Purpose Scope Policy Statement Definitions | 1 |
| Categories of Individuals | 2 |
| Categories of Data Overseas Data Transfer The Six Principles of GDPR | 3 |
| Process for Request | 13 |
| Process for Reasons of Legal Duty Responsibilities | 14 |
| Breaches of Policy | 15 |

Introduction

The Staffordshire Pension Fund manages the pension records of over 100,000 pension scheme members. The Fund is not a legal entity in its own right, it sits as a function of Staffordshire County Council who hold the capacity of Administering Authority.

The Council, and therefore the Fund, are classed as a Data Controller under the General Data Protection Regulations (GDPR) and the Data Protection [bill] 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 Data Protection legislation.

1. Purpose

The purpose of this policy is to define the Fund's responsibilities under GDPR, 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 GDPR in our working practices and to provide an overview to Fund officers of how GDPR should be applied to inform their decisions and day to day work by providing a legal background to the processing of personal data.

2. Scope

This policy applies to all employees, officers, Pension Committee Members, Local Pension Board, Pension Consultative Forum, 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 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

3. Policy Statement

This policy sits within the Fund's Information Governance Framework. This policy will be reviewed on an annual basis as part of the information governance assurance program.

4. 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 Staffordshire Pension Fund is a data controller.
- f) 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 Staffordshire Pension Fund is the Staffordshire County Council Information Governance Officer.
- g) Data Protection Officer (DPO)** – Is the designated person within an organisation that has responsibility for ensuring 'legal' compliance with GDPR, which relates only to personal data. The DPO for the Staffordshire Pension Fund is the Staffordshire County Council Information Governance Officer.

5. Categories of Individuals

The Fund, in providing pension benefits to its members, categorises its membership in 3 distinct profiles

- 6.1 Active Members
This relates to members of the Fund who are in current employment with a Fund employer and are contributing to their pension benefits. The Fund distinguishes these members from other categories of data as the personal data held by the Fund is jointly-controlled by the Fund and the Employer.
- 6.2 Deferred Members - employed
This relates to members of the Fund who are employed by a Fund employer and who in the past have contributed to their pension benefits but have chosen not to currently continue contributing to their pension benefits. The Fund is a joint data controller with the employer for these individuals.
- 6.3 Deferred Members – no longer employed
This relates to members of the Fund who are no longer employed by a Fund employer, but who have retained their pension account. 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.
- 6.4 Pensioner Members
These are members who are in receipt of their pension benefits. The Fund is the data controller for these members.

- 6.5 Beneficiary Pensioners
These are members who have inherited pension rights from their spouse or family member. The Fund is the data controller for these members.
- 6.6 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 Schedule 1 (16) of the Data Protection [bill] as the holding of the information is necessary for the purpose of making a determination in connection with eligibility for pension benefits.

6. Categories of Data

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

- 7.1 Special categories of data
This relates to sensitive personal information as defined in the GDPR 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 on entitlement of benefits in line with the regulations.
- 7.2 Personal data
This relates to data about an individual which is not classed as a special category of data and can include information relating to contracts of employment and salary.
- 7.3 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 entitlement.
- 7.4 Employer data
This is information relating to the Fund's employers for who the Fund may hold individual officer contact details.

7. 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.

8. The Six Principles of GDPR

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

| Principles | Fund position |
|--|---|
| <p>1. Processed lawfully, fairly and in a transparent manner in relation to individuals.</p> | <p>The Fund provides pension benefits to over 100,000 members who are automatically enrolled into the fund on commencing their employment with an eligible employer.</p> <p>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 of the Fund.</p> <p>The new joiner's information pack contains details of the Fund's Information Governance Policy, including directing members to the Fund's Privacy Notice (FPN) confirming how their information is used, and with whom it is shared.</p> <p>The member's rights are also outlined in the FPN and provide details on how a member can ask questions or request information relating to these rights.</p> |
| <p>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.</p> | <p>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 hold which they may choose to amalgamate. This information is required by statute in order to process a member's pension account.</p> <p>The Fund, reviews the data to review 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.</p> |

| | |
|---|--|
| | <p>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.</p> |
| <p>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.</p> | <p>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 is holds is specific and relevant for the purposes it was collected.</p> <p>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.</p> |
| <p>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</p> | <p>The Fund has a Pensions Portal, a self-service platform for members of the Fund to obtain details of their pension benefits and log into their own account to check and update their details. This platform serves as a useful tool for ensuring the information held about members is accurate.</p> |

| | |
|--|--|
| | <p>The Fund undertakes a regular tracing program for deferred members to ensure the information we hold is accurate at the point of retirement.</p> <p>The Fund has published a FPN which outlines a member's rights to request rectification of their data and how to make this request.</p> |
| <p>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; 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 by the GDPR in order to safeguard the rights and freedoms of individuals.</p> | <p>The Fund, in providing statutory duties under the 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 record of basic member details but will endeavour to delete any other information including any documents relating to the member. 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.</p> |
| <p>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.</p> | <p>The Fund, is part of the Councils, Data Security Policy , which outlines how the Fund protects members' data</p> <p>When contracting with third parties (as outlined in the FPN) the Fund requires all service providers to enter into a data sharing agreement, which sets out the Fund's expectations of the service provider in its protection of information and required confirmation by the service provider that are conversant with their duties under GDPR and are able to comply with them.</p> <p>When engaging with members, the Fund has implemented a 3 stage identity check process which requires members to pass 3 identification questions when contacting the Fund</p> |

Article 5(2) of the GDPR requires that ‘the controller’ (ie. The Fund) shall be responsible for, and be able to demonstrate, compliance with the principles.

This policy aims to meet that requirement.

6.1 Lawfulness of processing conditions

Under GDPR, 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 table below sets out the lawful basis for processing personal data and how the Fund manages members’ data in line with this.

| Condition | Fund position |
|---|---|
| 6 (1) (a) Consent of the data subject | <p>The Fund, as a Local Government Pension Scheme Fund provides statutory pension benefits to all its members.</p> <p>Members are automatically enrolled into the Fund through their employment contract and have the option to opt-out once in employment.</p> <p>While it may be argued that individuals do not consent to their data being held by the Fund, it is a statutory requirement to automatically enroll eligible members into the scheme.</p> |
| 6 (1) (b) Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract | <p>As a statutory scheme, there is no formal contract with individual members, however the statutory duty to provide pension benefits to eligible employees could create a binding agreement.</p> |
| 6 (1) (c) Processing is necessary for compliance with a legal obligation | <p>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.</p> |

| | |
|--|---|
| <p>6 (1) (d) Processing is necessary to protect the vital interests of a data subject or another person.</p> | <p>As a pension provider, the Fund may hold details of a member’s next of kin/family member/associate whose details it will hold for the purpose of beneficiary pensions and/or death grant nominations. The information 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 at some point in the future.</p> |
| <p>6 (1) (e) 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.</p> | <p>The Fund, as a Local Government Pension Scheme Fund provides statutory pension benefits to all its members and may rely on this condition when processes member data.</p> |
| <p>6 (1) (f) Necessary for the purposes of legitimate interests pursued by the data controller.</p> | <p>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.</p> |

8.2 Special conditions for sensitive personal data

In addition to the above conditions, where an organisation processes sensitive personal data, it must also comply with Article 9 of the GDPR. The table below sets out how the Fund complies with this Article

| Condition | Fund position |
|---|--|
| <p>9 (2) (a) Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State Law</p> | <p>The Fund, as a Local Government Pension Scheme Fund provides statutory pension benefits to all its members. Members are automatically enrolled into the Fund through their employment contract and have the option to opt-out once in employment.</p> <p>While it may be argued that individuals do</p> |

| | |
|---|---|
| | not consent to their data being held by the Fund, it is a statutory requirement to automatically enroll eligible members into the scheme. |
| 9 (2) (b) 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 may rely on this condition when processes member data. |
| 9 (2) (c) 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 may rely on this condition when processing the sensitive data of those members and their families. |
| 9 (2) (d) 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 |
| 9 (2) (e) 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. |
| 9 (2) (f) Processing is necessary for the establishment, exercise or in defence 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 Process and may require the retention of personal data to defend such claims. |
| 9 (2) (g) 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. |
| 9 (2) (h) Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working | This condition is not relevant to the work of the Fund. |

| | |
|---|---|
| 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. | |
| 9 (2) (i) 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. |
| 9 (2) (j) Processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with the GDPR. | This condition is not relevant to the work of the Fund. |

6.4 Individuals' Rights

One of the key obligations on organisations who manage and control individuals' data is to ensure the individual is informed about their rights under GDPR which gives them control over how their information is used and by whom.

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 will publish on its website a Fund Privacy Notice which outlines what personal information the Fund will hold, who it will share it with and for how long the information will be held.

Should an individual feel that the information supplied in the Fund Privacy Notice is inadequate or that it doesn't inform them about the how their information is used by the Fund, please the contact Staffordshire County Council's Information Governance Officer for more information.

b) The right of access

This is an individual's right to obtain

- confirmation that data is being processed

- access to personal data
- access to policies and information held by the Fund about how it uses data

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 pensions.enquiries@staffordshire.gov.uk

Copies of the information held will be provided within one month of receiving a request, however should a request be more complex, the Fund may write informing that your request may take longer confirming the date when the information will be provided.

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 pensions.enquiries@staffordshire.gov.uk and we will amend the information accordingly.

The Staffordshire Pension Fund operates a self service platform where members can amend details the Fund holds about them, including their address. Members are encouraged to use this platform to ensure the information the Fund holds about them is accurate and up to date.

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 (ie otherwise in breach of the GDPR).
- The personal data has to be erased in order to comply with a legal obligation.

The Fund, in providing statutory duties under the regulations has determined that it cannot permanently delete a member's record. Should a member transfer out of the, the Fund will retain a pension but will endeavour to delete any other information including any documents relating to the member. 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.

e) The right to restrict processing

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

A request for information to be used for limited purposes will not delete the information the Fund holds.

The Fund publishes a Fund 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 pensions.enquiries@staffordshire.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 pension provider. The Fund will provide the information it holds to a new pension provider in a format that they can use. The transfer would not take place without your consent.

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, for example where we outsource our print to mail documents (payslips, P60's, benefit statements). Under GDPR 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. In cases such as this the Fund will take appropriate 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

The General Data Protection Regulations 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 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 Fair Processing Notice has been written in a way they can understand.

9. Process for requests

Where an individual data subject has a question or complaint regarding how their rights under GDPR are upheld, they are encouraged to make contact in writing (email) to the Staffordshire County Council information Governance Officer in the first instance.

Data subjects who consider that 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. 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.

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 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 Customer Feedback Policy.

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.

10. Process for reasons of legal duty

The Fund may receive requests for information from various sources. This can include court orders, or requests under Section 29 (Crime & Taxation) or <Section 35 (Legal Proceedings) of the Data Protection Act 1998 (to be superseded by EU General Data Protection Regulation in May 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 regularly review Data Sharing Agreements when sharing information with Joint Data Controllers. The Fund will ensure that appropriate contracts and data processing agreements are in place when using third party contractors as data processors. All of the Fund's data sharing and data processing arrangements 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 Information Sharing Policy.

11. Responsibilities

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

The Fund will 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 will implement a process to ensure all staff handling personal information 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 GDPR awareness training and more in depth training if they are involved in the processing of personal data.

The Fund will monitor and review its processing activities to ensure these are consistent with the principles and individual rights under GDPR legislation and will ensure that its notifications are kept up-to-date.

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 appropriate Privacy Notices are maintained to inform data subjects of how their data will be used. These will be assessed in line with the Privacy Impact Assessment.

The Fund will review and update this policy to ensure it remains consistent with the Law, and any Compliance Advice and Codes of Practice issued by the ICO.

12. 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 the GDPR.

The GDPR 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 members, partner agencies, contractors and vendors have a responsibility to report security incidents and breaches of this policy as quickly as possible through the Fund's Incident Reporting Procedure. 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 Senior Fund management and the Information Governance Unit of Staffordshire County Council.

Document Control Information

| | |
|----------------|--|
| Document title | General Data Regulation Protection Policy |
| Owner | Staffordshire Pension Fund / Staffordshire Information Governance Unit |
| Service Area | Treasury & Pensions |
| Approved by | Melanie Stokes – Head of Treasury & Pensions |

Contacts

| | |
|-------------------------|---|
| Data Protection Officer | Staffordshire County Council Information Governance Unit (01785) 278314 |
| General Fund enquiries | (01785) 278222 |