DATA STRATEGY POLICY

TRUSTEES OF THE j murphy group pension plan

January 2018

Contents

1. Introduction 3

Background 3

Role of Trustee 3

PURPOSES FOR WHICH DATA are PROCESSED 3

Categories of personal data processed 4

Data Subjects 4

Legal basis OR BASES for processing personal data 5

data protection PRINCIPLES 5

2. TRUSTEE policy 7

3. PROCESSORS / service providers and sharing data with other third parties 9

Appointing a new processor and/or other service provider 9

Processors / service providers 9

trustee criteria for processors / service providers 10

sharing data with third parties 11

4. DATA RETENTION 12

5. Personal data breach 13

Definition of a personal data breach 13

identification of a personal data breach 13

Personal data breach management 13

*Likely to result in a risk to the rights and freedoms of natural persons* 13

*Likely to result in a high risk to the rights and freedoms of natural persons* 14

*Documentation and remedial action* 14

6. Conduct and proceedings 15

APPENDIX - GLOSSARY OF IMPORTANT GDPR TERMS 16



* 1. Introduction

This Policy sets out the rules adopted by the Trustees of the J Murphy Group Pension Plan (the Trustee) in respect of data protection and the conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of personal information. It also includes protocols for the conduct of trustees and their proceedings.

The Policy, the inventory of processing activities (see below) and risk register (see **Section 2**) are reviewed by the Trustee at least annually and following any material changes that may impact the processing of the personal data for which they are responsible and any material change to legislation or guidance.

The Trustee will seek its own independent legal advice as appropriate.

Date of last review: March 2023

# Background

The Trustee is responsible for the capture, maintenance, processing and security of all personal data held as part of the J Murphy Group Pension Plan (the Plan) and necessary for the administration and management of the Plan.

The Trustee responsibilities are significant and are governed by, inter alia, Trust and Pensions Law, the Rules of the Plan, the General Data Protection Regulation (GDPR) and, when it receives Royal Assent and comes into force, the Data Protection Bill (references to GDPR in this document should, where appropriate, be interpreted as including any legislation that replaces it).

In developing this Policy, the Trustee has considered relevant law and practice in relation to the processing of personal data in the context of pension schemes.

The objective of the Policy is to provide a framework that will assist in compliance with data protection obligations in relation to Plan personal data, not just by the Trustee but also its delegated authorities including, where appropriate, the sponsoring employer(s) of the Plan (the Sponsor).

# Role of Trustee

The Trustee is a Data Controller in respect of the Plan.

# PURPOSES FOR WHICH DATA are PROCESSED

The processing for which the Trustee is responsible and the purposes for which it is generally undertaken are described in the following table.

|  |
| --- |
| **Purposes for which personal data is processed** |
| Occupational pension scheme administration, including payment of benefits to and in respect of pension Plan members and beneficiaries on leaving service, retirement and death; communication with members and other beneficiaries; financial reporting; and investment of assets.In more detail, processing activities in respect of members, beneficiaries and other data subjects include but are not restricted to – * Issuing communications and information
* Responding to queries and disputes
* Calculation and payment of benefits (including pensions, lump sums and transfer values)
* Establishing eligibility for benefits
* Calculation and reconciliation of contributions
* Payment of tax charges and monitoring whether pension tax allowances are exceeded
* Reporting to HMRC
* Ensuring compliance with contracting-out requirements
* Preparation of Plan financial statements and other returns
* Actuarial valuations, updates and calculations
* Investment of pension Plan assets
* Obtaining or preparing quotes for annuities or other insurance contracts
* Purchasing annuities or other insurance contracts
* Managing pension Plan risk
* Exercising Trustee powers and discretions
* Carrying out any other activity which is incidental to the performance of Trustee duties in relation to the Plan
 |
| Occupational pension Plan payroll, including payment of pensions to members and beneficiaries and accounting to HMRC for tax on pensions |
| Group Life Assurance administration, including the renewal processing, re-broking exercises and managing claims |

# Categories of personal data processed

The categories of personal data that the Trustee processes are described in the following table.

|  |
| --- |
| **Categories of personal data processed** |
| Personal attributes : Name; address, Age or date of birth; identifier(s); marital information (including divorce); gender; employment history; remuneration information; National Insurance Number; PAYE information; bank account details  |
| Special Categories of Data : Health information; medical diagnosis information; race or ethnic origin; sexual orientation; religious / philosophical / political beliefs; membership of trade union |
| ‘Other’ Plan membership information, including details of pension contributions and benefits; nomination forms (which are sealed until death); and adviser / service provider details |

# Data Subjects

The Data Subjects to which this Policy applies include all of the Plan beneficiaries and other individuals in the table below.

|  |
| --- |
| **Categories of data subjects** |
| Active members of the Plan to which this policy applies |
| Members who have left the Plan, including those who have transferred out or have otherwise ceased to have benefits secured or payable under the plan |
| A pensioner who is drawing a pension or other form of benefit from the Plan |
| A contingent beneficiary of any other above membership categories e.g. a child or adult dependant |
| Anyone acting on behalf of a deceased member of the Plan e.g. a family member or friend of the deceased |
| A legal representative of a member of the Plan |
| An Independent Financial Adviser formally appointed by a member of the Plan |
| Members who have transferred out or taken a refund |

# Legal basis OR BASES for processing personal data

The Trustee is responsible for ensuring that it has an appropriate legal basis for the processing of Plan personal data as identified in the GDPR. The Trustee’s legal basis for processing personal data may vary according to data subject, category of data held and / or purposes for which it is used.  In some circumstances more than one legal basis for processing personal data may apply to a particular category of processing.

The processing described above (other than the processing of special category data) is generally necessary for the legitimate interests of administering the Plan and related purposes set out above.  The Trustee has carried out an assessment and does not consider that this processing will prejudice the interests, rights or freedoms of the data subjects.

The Trustee also processes personal data to fulfil its legal obligations under the Pensions Acts and the Plan’s governing documentation.

Explicit consent is obtained for the processing of special category data. Consent may also be used as a basis for processing personal data in other circumstances.

The specific basis or bases for processing the different categories of personal data processed by the Trustee is set out in the table below.

|  |  |
| --- | --- |
| **Categories of personal data processed** | **Legal basis or bases** |
| Personal attributes : Name; address, Age or date of birth; identifier(s); marital information (including divorce); gender; employment history; remuneration information; National Insurance Number; PAYE information; bank account details  | Legitimate Interest and Legal Obligation |
| Special Categories of Data : Health information; medical diagnosis information; race or ethnic origin; sexual orientation; religious / philosophical / political beliefs; membership of trade union | Consent |
| ‘Other’ Plan membership information, including details of pension contributions and benefits; nomination forms (which are sealed until death); and adviser / service provider details | Legitimate Interest and Legal Obligation |

# data protection PRINCIPLES

The Trustee recognises that, in their role as Controller, they are directly responsible for compliance with all aspects of the GDPR and for demonstrating compliance in respect of the Plan. They recognise that if this is not achieved then a liability to pay damages may arise, and the Trustee could be subject to fines or other penalties and / or sanctions.

The Trustee is responsible for and must demonstrate compliance with the GDPR principles. The GDPR principles are:

* **Lawfulness, fairness and transparency:** data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.
* **Purpose limitation:** data must be collected for specified, explicit and legitimate purposes and not processed in a manner incompatible with those purposes.
* **Data minimisation:** data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
* **Accuracy:** data must be accurate and, where necessary, kept up to date. Reasonable steps must be taken to ensure that inaccurate personal data are erased or rectified without delay.
* **Storage limitation:** data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data are processed.
* **Integrity and confidentiality:** processing must ensure appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.



* 1. TRUSTEE policy

| **Issue** | **Policy** |
| --- | --- |
| **Data strategy approach** | The Trustee has taken and will continue to take independent legal advice on the application of GDPR to the Plan where applicable.The Trustee has obtained input from the processors it has contracted with to provide services to the Plan, and provides instruction to those processors in respect of the Trustee’s approach to GDPR.The Trustee has added GDPR to its ‘Trustee Knowledge and Understanding’ (TKU) requirements for trustee training.The Trustee has put in place protocols in relation to conduct and proceedings (**Section 6**). |
| **Data Protection Officer** | The Trustee is not required to appoint a Data Protection Officer. |
| **Data Protection Impact Assessments** | The Trustees is aware of the requirements for Data Protection Impact Assessments (DPIAs) and the forms of processing which may trigger DPIAs. DPIAs will be carried out where required by the GDPR. |
| **Records of processing activities** | The Trustee maintains a record of processing activities in line with the requirements of GDPR.  |
| **Privacy notices** | The Trustee is responsible for the content and issue of privacy notices in line with GDPR. |
| **Consent** | The Trustee will obtain, record and monitor the explicit consent from data subjects to process any special category personal data. For data other than special category data, the legal basis / legal bases for processing is / are described in Section 1. |
| **Data Subject Rights** | The Trustee recognises the rights of the data subject as set out in the GDPR including:* Their right of access to information
* Their right to have information corrected or updated
* Their right to be forgotten
* Their right to restrict processing.

Trustee training on GDPR includes data subject rights.Data subjects wishing to exercise their rights are required to write to the Trustee (email or paper) setting out their request.Trustee will review the request within 5 working days to establish whether the request is valid. The Trustee will seek independent legal advice if necessary.On completion of the review, the Trustee will contact all relevant processors that need to support the request.Subject access requests must be responded to within a month.The Trustee is aware that, in certain circumstances, legislation allows personal data to be disclosed without the consent of the data subject. The Trustee acknowledges that, in certain circumstances, personal data will be disclosed without such consent or even knowledge of the data subject. The Trustee will ensure that its processors are obliged to comply with the rights of data subjects as set out in the GDPR.The Trustee will assess the impact of new rights on the Plan and up-date these policies accordingly. |
| **Privacy by Design and Default** | Compliance with data protection regulation is proactively taken into account when designing or reviewing processes and applications that affect personal data. The Trustee will review the AAF/001 report provided by Mercer annually as part of the process of assessing Mercer’s compliance with the GDPR. Additional audit tests may be carried out as appropriate. |
| **Supply chain management** | See **[Section 3]**. |
| **Personal data security** | The Trustee will implement appropriate technical and organisational measures in respect of personal data security. These will include:* Processes for regularly testing, assessing and evaluating the effectiveness of security measures
* Measures to guard against the risks of accidental or unlawful destruction of personal data, data loss or alteration and unauthorised disclosure of, or access to, personal data, and obligations to notify the Trustee promptly of any such events occurring
* Measures preventing the processing of personal data other than on the explicit instructions of the Trustee.

See also **[Section 6].** |
| **Transferring personal data outside the EEA** | The Trustee will require any processor who transfers personal data outside the EEA to put in place appropriate safeguards(\*) before doing so, such as use of model clause agreements that have been approved by relevant regulators. (\*) Including but not restricted to – * Not transferring personal data outside of the EEA until appropriate checks have been made
* Ensuring administrators have processes in place to consider data protection whenever a Plan member or beneficiary requests an overseas transfer.
 |
| **GDPR compliance monitoring** | Risks in relation to data protection and GDPR are recorded and reviewed on the Trustee risk register.The Trustee has included GDPR within its audit scope to test compliance.The Trustee includes data protection as a standing agenda item under governance at its meetings, including the review of management information regarding data subject rights, breaches and developments in legislation, Regulator guidance and best practice.The Trustee seeks governance advice and practical assistance in reviewing risk and compliance. |



* 1. PROCESSORS / service providers and sharing data with other third parties

This section sets out the Trustee’s policy regarding the use of processors and other service providers as well as its policy regarding the sharing of personal data with other third parties.

# Appointing a new processor and/or other service provider

As part of the appointment of individuals and organisations, the Trustee will require them to provide a written statement of compliance with the GDPR and the Trustee’s specific requirements for the Plan. In particular, service providers will be required to demonstrate how they keep data secure and how they test their security arrangements.

All service providers must enter into a contract for services with the Trustee, which will include specific GDPR requirements.

In addition, each contract with a processor will comply with Article 28 of the GDPR and include, inter alia, the following provisions.

Processors must:

* process personal data only on documented instructions from the controller;
* ensure that persons authorised to process the personal data have committed themselves to confidentiality;
* take all measures required by GDPR regarding the security of processing personal data;
* assist the controller’s obligation to respond to requests for exercising the data subject’s rights and managing personal data breaches.

Further, each contract between the Trustee and its processors must set out:

* the subject-matter and duration of the processing,
* the nature and purpose of the processing,
* the type of personal data
* the categories of data subjects and
* the obligations and rights of the controller.

# Processors / service providers

The organisations and individuals which process personal data in the course of providing services to the Trustees or who process personal data as data processors for and / or on behalf of the Trustee are listed below.

|  |  |  |  |
| --- | --- | --- | --- |
| **Position** | **Name** | **Capacity** | **GDPR contract in place (Y/N)** |
| Sponsoring employer(s) | J Murphy and Sons | Controller | N/A |
| Current Scheme Actuary | Ashleigh Harwood | Controller | Yes |
| Scheme Administrator | Mercer  | Processor | Yes |
| Scheme Auditors | Planet Audit LLP | Controller | N/A |
| Legal Adviser | Stephenson Harwood LLP | Controller | N/A |
| Investment Managers | Schroders | Processor | To be signed |
| Investment Consultant | Schroders | Processor | To be signed |
| Custodian | Citibank, BNY Mellon | Processor | N/A |
| AVC provider - DB | Phoenix LifeAviva | Controller | N/A |
| Annuity Provider | JUST (formerly Partnership) | Controller | Yes |
| Insurer(s) of specific benefits e.g. life assurance, death-in-service pensions, disability benefits and salary replacement schemes | Canada Life | Controller | N/A |
| Bank | RBS | Controller | N/A |
| Printer / Communications provider | Primedoc | Mercer Sub-processor | Yes |
| Member tracing provider | Lexis Nexis | Mercer Sub-processor | Yes |
| Archiving Service Provider | Iron Mountain | Mercer Sub-processor | Yes |

# trustee criteria for processors / service providers

| **Requirements** | **Comments**  |
| --- | --- |
| **General** | The Trustee requires confirmation that staff have been trained in the requirements and behaviours necessary to be compliant with the GDPR.The Trustee requires processors to advise it of all changes in approach which may affect GDPR compliance so that the Trustee can, where necessary, provide instruction. |
| **Records of processing activities** | The Trustee requires confirmation that a record of processing activities is maintained in line with the GDPR requirements. |
| **Privacy by Design & Default** | The Trustee requires regular confirmation, at least every year, that data protection regulation is proactively taken into account when designing or reviewing processes and applications that affect personal data.The Trustee will discuss and agree the introduction of additional audit tests as required to assess compliance with the GDPR. |
| **Data Protection Impact Assessment (DPIA)** | Where the requirement for a DPIA applies, confirmation will be provided that one has been undertaken. |
| **Data Protection Officer** | Where the requirement for a data protection officer applies, their name and contact details will be provided. |

# sharing data with third parties

The Trustee will only provide personal data to third parties who request access to Plan personal data where it has determined that the party in question it is entitled to do so under the GDPR and in a manner compliant with the GDPR. Parties that personal data may be provided to include, but are not limited to, the following:

* Her Majesty’s Revenue and Customs (HMRC)
* The Pensions Regulator
* The Pensions Ombudsman
* Department for Work and Pensions
* The Pensions Advisory Service
* The Courts
* The Police

Data may be shared with the Sponsoring employer(s) provided there is a legal basis or bases for sharing it.

The Trustee will always document the legal basis or bases relied upon whenever data is shared with a third party, including the Sponsor employer(s).

For subject access requests, see **Section 2**.



* 1. DATA RETENTION

Pensions are long-term benefits in that members build up their benefits over very long periods and can be drawing benefits for twenty years or more.

Additionally, it is not unusual for disputes to occur which require interrogation of Plan data going back decades.

The Plan’s data are held in a number of different ways by the Trustees and different delegated authorities / service providers, and for different periods and reasons.

However, Plan data will be held only for so long as is necessary for the proper and compliant governance and administration of the Plan. Where data is no longer required, it will be destroyed in a manner that ensures it is put permanently beyond use; e.g. -

* Where data is held in a paper format, destruction means that the data will be shredded.
* Where data is held by third parties, the Trustee will rely on confirmation from them that data has been destroyed.

The maximum periods that the Trustee will normally hold / process personal data are as follows –

* For so long as any benefit is secured or payable under the Plan to or in respect of a member or beneficiary, the Trustee we will retain so much of their personal data as is necessary to ensure that benefits can be paid correctly
* Where benefits cease to be payable or secured under the Plan, e.g. in the case of transfer-out, a pension benefit buy-out or benefits being otherwise discharged, the Trustee will continue to hold such personal data as the Trustee considers is necessary to fulfil the purposes of the Plan as set out in Section 1 and / or deal with any complaint or dispute in relation to any benefit entitlement.
* The Trustee will never process or hold on to data for longer than the life of the Plan plus 15 years.



* 1. Personal data breach

# Definition of a personal data breach

A personal data breach means a breach of security or other incident leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

# identification of a personal data breach

All processors are required by contract to report any personal data breach to the chair of the Trustee (or nominated deputy if he/she is not available for any reason) within 24 hours of that breach being identified.

Any Trustee that is made aware of a personal data breach must inform all other Trustees within 24 hours of that breach being identified.

All Trustees receive training at least once a year on how to identify a personal data breach.

The Trustee has implemented measures to detect potential personal data breaches. These include:

* Requiring Processors to inform the Trustee of a data breach as soon as practicable possible after they have become aware of it.
* Taking into account guidance issued on data breach handling by the ‘Article 29 Working Party’ (the EU data protection advisory body).

# Personal data breach management

The Chair of the Trustee and at least one other Trustee must review the breach and, taking into account guidance from the Article 29 Working Party (such as the Guidelines on Personal data breach notification under Regulation 2016/679) or Information Commissioner’s Office on data breach handling, determine whether the breach is:

* Unlikely to result in a risk to the rights and freedoms of natural persons. Examples include:
	+ The Trustee has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption
* Likely to result in a risk to the rights and freedoms of natural persons.
* Likely to result in a high risk to the rights and freedoms of natural persons.

The outcome of this review must be documented.

The Chair of the Trustee may call an exceptional Trustee’s meeting to discuss the breach.

The Chair of the Trustee should consider the appointment of legal adviser taking into account the severity of the breach.

# *Likely to result in a risk to the rights and freedoms of natural persons*

If the breach is likely to result in a risk to the rights and freedoms of natural persons then Trustee must without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the ICO.

Where the notification to the ICO is not made within 72 hours, it shall be accompanied by reasons for the delay.

Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

The notification to the ICO shall include as a minimum:

* Description of the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
* The name and contact details of the nominated contact where more information can be obtained;
* Description of the likely consequences of the personal data breach;
* Description of the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

# *Likely to result in a high risk to the rights and freedoms of natural persons*

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

The communication to the data subject shall describe in clear and plain language the nature of the personal data breach and contain at least:

* The name and contact details of the data protection officer or other contact point where more information can be obtained;
* Description of the likely consequences of the personal data breach;
* Description of the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

The communication to the data subject shall not be required if any of the following conditions are met:

* The Trustee has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise;
* It would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

# *Documentation and remedial action*

The Trustee shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken (both in respect of the breach and to reduce the risk of a further occurrence).

All processors are required by contract to support the root cause analysis and remedial action where appropriate.



* 1. Conduct and proceedings

This section sets out the Trustee’s policies on data security in the context of the conduct and proceedings of members of the trustee board.

In particular -

* All Trustee Papers are sent by secure means.
* Trustees do not include personal information in emails. Any emails containing personal information are sent by secure means.
* Members of the Trustee board have a Sponsor based e-mail within the organisations firewall.
* Data security is included in the trustee knowledge and understanding (‘TKU’) programme.
* Retiring members of the trustee board confirm all personal data held as a board member has been destroyed.
* In the event of a data security breach, the Trustee has a communication protocol in place.
* When the Trustee transfers data to another party, measure are in place to ensure that the transfer is made in a manner that keeps data secure.

APPENDIX - GLOSSARY OF IMPORTANT GDPR TERMS

|  |  |
| --- | --- |
| Personal data | Information relating to an identifiable person. Note that a person may be identifiable in many different ways and that the definition extends to data that could be linked to a specific individual by use of other data in the possession or control of the Trustees or their processors and also data that they may be able to obtain from public sources. |
| Special category [formerly sensitive] data | Reveals racial or ethnic origin; political opinions; religious or philosophical beliefs; trade-union membership; data concerning health or sex life and sexual orientation; genetic or biometric data. |
| Processing | Operations performed on personal data. This is very wide ranging as it captures anything that can be done with data and includes simply storing it, accessing it and deleting it. |
| Controller | Body that determines the purpose and means of the processing of the personal data.Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. |
| Processor | Body that carries out processing on behalf of the controller. |
| Data Subject | A natural person whose personal data are processed by a Controller or Processor. |
| Data Protection Impact Assessment | Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks. |
| Privacy by Design and Default | This concept can be best described, in a GDPR context, as ensuring that compliance with data protection regulation is not an after-thought but proactively taken into account when designing or reviewing processes and applications that affect personal data. |

CONTACT

The Trustees of the J Murphy Group Pension Plan

Hiview House

Highgate Road

London

NW5 1TN

Appointed Scheme Actuary

Mercer

Belvedere

12 Booth Street

Manchester

M2 4AW