AMG UK Group 2006 Pension Plan
Trustee's data protection policy

Note: *Definitions of the key terms used in this Policy are set out in* ***Appendix 1****.*

The Trustee of the AMG UK Group 2006 Pension Plan (the "**Scheme**") is the **controller** for the purposes of data protection laws applicable in the UK, which include the United Kingdom General Data Protection Regulation ("**UK GDPR**") and the Data Protection Act 2018. We will refer to 'Data Protection Legislation' in this policy and that term is defined in Appendix 1.

This document sets out the approach the Trustee will take to comply with its legal obligations in relation to the Member and Beneficiary data that they hold.

The Trustee of the Scheme is the AMG Group UK Pension Trustee Limited. Its contact details are:

Christine Allen
AMG Chrome Limited
Fullerton Road
Rotherham
South Yorkshire S60 1DL
Tel: 01709 833 754
Email: payroll@amg-chrome.com

Any questions about this data protection policy should be addressed to:

Leonora Scaife
AMG Chrome Limited
Fullerton Road
Rotherham
South Yorkshire S60 1DL
Tel: 01709 833 754
Email: lscaife@amg-chrome.com

So that the Scheme can be run properly and we can pay the promised benefits, we pass data to other parties, some of whom are joint controllers with the Trustee and some of whom are our processors. Details of these other parties and how they can be contacted are set out in our Data Record. A copy of this is available from Leonora Scaife.

In this policy, unless otherwise stated, "we", "us", and "our" are used to refer to the Trustee in its capacity as controller.

1. WHY WE HOLD INFORMATION AND WHAT IT IS USED FOR

1.1 General

We hold personal data about Members and Beneficiaries (see Section 2 for details about what kind of information we have). We need this information to ensure that correct contributions are paid and that benefits are correctly calculated, and are paid at the right time and to the right person.

We require sufficient information to:

- determine the level of contributions that should be paid into the Scheme by and on behalf of Members;
- calculate all benefits payable from the Scheme;
- communicate with Members and Beneficiaries;
- manage risk appropriately under the Scheme (which may include the purchase of insurance contracts);
- determine when benefits should be brought into payment;
- exercise any powers and discretions we have in relation to the Scheme; and
- carry out any other activity which is incidental to the performance of our duties in relation to the Scheme.

1.2 Lawful reason

Data protection law requires us to process any personal data fairly and lawfully. This means that we must have a "lawful reason" for processing Member and Beneficiary data from a list set out in Data Protection Legislation. Additional lawful reasons are needed if special categories of personal data or data relating to criminal convictions or offences are processed.

We rely on several lawful reasons for processing personal data, depending on what we are doing. For instance:

- *Processing is necessary for the purposes of the legitimate interests pursued by the Trustee or by other parties (such as the Scheme employers)*. We have a duty to administer the Scheme properly and pay benefits as they fall due. To do this, we need to process personal data relating to Members and Beneficiaries for our legitimate interests. Members and Beneficiaries have the right under Data Protection Legislation to object to their personal data being processed when we rely on legitimate interests. We consider that the need to ensure that Members and Beneficiaries get the promised benefits from the Scheme is an important legitimate interest, and that whilst Members and Beneficiaries have the right to object, we will usually be able to show that our legitimate interests are compelling and that those legitimate interests are not overridden by the rights and freedoms of the Members and Beneficiaries. As for our legitimate interest in sharing personal data with other parties, this might include (for example) insurers who receive data in a buy-out/buy-in scenario, and such sharing would usually be for our legitimate interests, provided that it is necessary to share personal data instead of anonymised data.
- *Processing is necessary to comply with the Trustee's legal obligations to pay the benefits promised under the Scheme's governing documentation or with obligations imposed by statute.* For instance, regulations require that we obtain certain personal data from Members who wish to exercise their statutory right to transfer benefits to another pension scheme.
- *Consent* (in very limited circumstances, for example when we obtain explicit consent to use special categories of personal data). Further details are in Section 1.3.

1.3 Consent to processing

We may rely on Members or Beneficiaries having consented to us processing their data for a specific purpose. This is usually only relevant to what we do with special categories of personal data, such as health information. Whilst sexual orientation details (which could be inferred from details we hold about same-sex, or indeed opposite-sex partners/spouses of Members where, for example, they are named on death benefit nomination forms) are a special category of personal data, it is rarely relevant to seek consent to hold it as long as we only hold and use it in necessary legitimate and expected ways (and not e.g. for any profiling of our membership). The same is likely to be true of any special category information or gender reassignment, including information relating to gender recognition certificates.

The circumstances where we may rely on consent are generally:

- where we are considering medical information in the context of an application for ill-health early retirement or a serious ill-health lump sum; or
- where we receive personal information in relation to payment of a death benefit lump sum (for example, on a death benefit nomination form).

Consent has a specific meaning under Data Protection Legislation. Where we rely on consent, we will ensure that it is:

- properly informed (Members or Beneficiaries will be told clearly what they are consenting to);
- clearly distinguishable from other matters in the same document (we will not 'bundle' several consents together or 'hide' them);
- intelligible, easily accessible and in clear and plain language; and
- where the information concerned relates to health or sexual orientation, explicit and relates to specific activities.

Our privacy notices and consent forms comply with Data Protection Legislation and we will instruct our Administrators to ensure that their notices and forms are similarly compliant.

We will also instruct our Administrators to maintain a record of each consent we rely upon – we must be able to demonstrate consent in this way to comply with Data Protection Legislation.

We will ensure that Members and Beneficiaries are told that they can withdraw consent. Where consent is withdrawn, processing of the relevant Member or Beneficiary data will cease immediately unless we are satisfied that there is an alternative lawful basis for processing that information. Our privacy notices clearly describe the consequences of withdrawing consent.

2. WHAT PERSONAL INFORMATION WE HOLD

2.1 Who we hold personal data about

We may hold personal data in relation to the following categories of people:

- Active Members;
- Pensioner Members;
- Deferred Members;
- Pension credit Members;
- Beneficiaries and potential Beneficiaries;

- Some former Members who no longer have any benefits or entitlements under the Scheme (for example, former Members who have transferred their benefits out of the Scheme).

2.2 Members

We will hold some or all of the following personal data about Members:

- Full name
- Date of birth
- Sex / gender
- Address and other contact details
- National Insurance number
- Salary information
- Details of benefits under the Scheme, including contributions paid, service dates and investment profile choices
- Bank account information
- Marital or civil partnership status (including divorce)
- Change of name details
- Death benefit nomination form
- Name of employer(s) (for Active Members) (or employer(s) when previously an Active Member of the Scheme, for Deferred or Pensioner Members) and employment history
- Data about a Member's personal relationships (see Section 2.4)
- Age at retirement
- Benefit entitlement data
- In certain circumstances, information regarding health (only obtained for the purpose of providing ill-health benefits or where it is relevant to a disability access need e.g. for communications to be in large text for visually-impaired Members) (see Section 2.4)
- Information relating to overseas residency, where a Deferred Member applies to transfer benefits to an overseas pension scheme
- Information (including service start date, name of employer and pay received) relating to employment with an employer participating in another occupational pension scheme, where a Deferred Member applies to transfer benefits to that scheme

2.3 Beneficiaries

We may also hold some or all of the following information about Beneficiaries who are being paid benefits from the Scheme in respect of a Member or who may be entitled to these benefits:

- Full name
- Date of birth
- Sex / gender

- Address and other contact details
- National Insurance number
- Bank account information
- Relationship to the Member
- Details of financial relationship with Member (where financial dependency is required as a condition of payment of a benefit)
- Data about the Beneficiary's health or personal relationships (see Section 2.4)
- Benefit entitlement data

2.4 Special categories of personal data and criminal convictions/offences data

From time to time, we will need additional data about a Member's or potential Beneficiary's health or personal relationships in order to determine their entitlement to ill-health or dependants' benefits. We may also need information about a potential Beneficiary's relationship with the Member to help us determine whether they are eligible for benefits. This could include information about their sexual orientation.

Similarly, information relating to a Member's or Beneficiary's gender recognition certificate may include special category personal data; and a Member or Beneficiary who does not hold such a certificate may also provide us with information on gender reassignment which includes such data if (for example) they tell us that they identify with a different gender from their birth sex, and that they would like our records and correspondence to reflect this fact.

We may also occasionally receive information about a Member's or Beneficiary's criminal convictions if the information is relevant either to their entitlement to a benefit or to a possible reduction to their benefits.

Where we are handling information in relation to an individual's health, we will generally seek explicit consent from that Member or Beneficiary.

In some cases, the law may allow us to process special categories of data without Member / Beneficiary consent where we have an alternative legal basis for doing so. If we are able to process such information without consent and choose to do so, we will comply with any additional legal requirements in relation to that processing. More information on this is set out in Appendix 2.

Where we are handling information in relation to criminal convictions and offences, we will ensure that we have a legal basis for doing so and that we comply with any additional legal requirements in relation to processing this data.

2.5 Review

The law requires that we only hold the information we need to run the Scheme properly and that we only use it for the purposes set out in Section 1 above. In our view, all of the information set out above is necessary for these purposes.

We will review the information that we hold periodically subject to a review being undertaken at least every three years to confirm whether it remains necessary for the purposes set out in Section 1.

We only collect information that we need to comply with our obligations in relation to the Scheme. We will keep data minimisation in mind when asking for information.

3. WHERE WE GET PERSONAL DATA FROM

The Scheme's participating employers provide us with information about a Member's salary and length of service.

We may receive names, addresses, national insurance numbers, bank account information and next of kin information from employers. This information may also be provided to us directly by Members.

Other information will be provided directly by a Member or Beneficiary to us (or our Administrators), such as information regarding how they would like their lump sum death benefit to be distributed, or information about medical conditions which may be relevant to the payment of benefits.

Where Members have transferred benefits in from other pension arrangements, we will receive personal information about them from the transferring scheme.

Where we are considering the distribution of or entitlement to death benefits, information will be provided to us by potential Beneficiaries, and may also be provided by those assisting in the administration of the deceased's estate.

Where we obtain personal data from a source other than the Member (such as the electoral roll), we will normally state this in our privacy notices and give additional information including the source of the data. However, in certain circumstances, such as where providing this information would involve disproportionate effort or seriously impair the objectives we are trying to achieve, we may not provide this information in our privacy notices.

4. WHO WE WILL SHARE PERSONAL DATA WITH

4.1 General

Our Data Record sets out details of the persons with whom we will share Member and Beneficiary data and the reasons why data may be shared. Copies of this are available on request from Leonora Scaife. This section of our Data Protection Policy is only intended to give an overview of why, and with whom, we share data.

The day-to-day operation of the Scheme is not carried out by the Trustee but by our Administrators. All the information about Members and Beneficiaries that we hold is passed to our Administrators.

At regular intervals, an actuary works out what the liabilities of the Scheme are worth and the assets and contributions that are required to meet them. To do this, the actuary needs information to work out what benefits are likely to be paid by the Scheme, and when. This means that the actuary needs the personal data the Trustee holds. However, they do not always need names and addresses to carry out their analysis and so, where possible, information is supplied to them on an anonymised basis.

We may require the services of an actuarial firm at other times where necessary to help us work out if we can reasonably agree to proposals from the employer and other strategic issues, or to determine the cost of particular benefits, or to generally assist us in the running of the Scheme. This may also require the processing of Member and Beneficiary data.

From time to time, the employer may wish to contact Members to explain options in relation to their benefits. The employer may require information from the Trustee to do this. Where we consider it appropriate, necessary and proportionate, and where that disclosure complies in all other respects with data protection law, we will supply the information to a relevant employer.

Your personal data may be passed onto third parties whom we work together with (including without limitation, iTrent, Aon, Mercer, Barnett Waddingham, Zurich, Eversheds Sutherland, BDO, AMG Advanced Metallurgical Group NV, Aviva, Prudential, Reassure and their associated companies and sub contractors) for providing us with services, such as payroll hosting, group life assurance, legal services, auditors and bulk annuity provider to support and maintain the framework of our pension scheme benefits.

Inevitably, we may need to share data with other people so that we can comply with our legal and contractual duties in respect of the Scheme, and in order to assist the employer in managing its relationship with its employees, and to ensure the efficient running and administration of the Scheme. We will share data where such sharing is necessary to meet these objectives.

In all cases, when sharing data with any third parties who are controllers in their own right we will need to consider the applicable requirements of the ICO's code of practice (see next section).

4.2 Sharing data – compliance with ICO Code of Practice

We are aware that we are expected to follow the statutory code of practice issued by the ICO when sharing personal data.

When sharing personal data with another organisation who also is an independent controller, in practice, this means that we must (among other things):

- have written terms in place with the other controller (eg. in a data sharing agreement);
- make sure we are satisfied that the other controller has common standards of security compared with those which we (or the Administrators as our processors) apply;
- be clear on what categories of personal data are being shared and for what purpose and what happens to those data once the recipient no longer needs them for that purpose;
- make sure we are satisfied that there is a legal basis justification for sharing the personal data with the recipient; and
- make sure that if health information or other special category personal data is shared there have been explicit consents for such sharing (unless an alternative legal basis justification applies).

When sharing personal data with another organisation who is a processor, under Data Protection Legislation we must include mandatory written terms in the contract with that organisation. In addition, the ICO expects that we have evidence showing that we have:

- carried out due diligence on that recipient before first sharing personal data with it, including on the security measures (not limited to cyber-security measures) in place at the recipient, so that we are confident that the recipient does in practice take appropriate steps to protect the personal data (in some cases we may use security questionnaires to this end);
- periodically revisited that due diligence during the contract term to check measures remain appropriate (again, this may mean that we use security questionnaires or replies to questions when calling for information using the rights contained in the contract); and
- ensured that a minimum list of technical and organisational security measures is included in the contract.

4.3 Transfer of data overseas

Where personal data is going to be involved in a 'restricted transfer' (i.e. a transfer to another country or territory to which transfers are prohibited under Data Protection Legislation unless extra steps are taken), we are responsible for ensuring that the personal data will be properly protected.

This includes, for instance, transfers from the UK to what are called 'third countries', which do not have adequate safeguards in their own laws to ensure the protection of personal data.

When we are asked to permit these of transfers e.g. by our Administrators if they wish to carry out their services using an office outside the UK, the following will apply.

Whenever we (or the Administrators) engage new processors, we (or they) will investigate at the outset of the engagement whether the nature of their operations involves a restricted transfer and, if so, on what mechanism transfers are based. We will not provide the new processors with any

personal data until we have received confirmation that satisfactory data transfer mechanisms are in place. We will ask for information about the safeguards that the recipient will apply to any personal data that is transferred.

As controller, we are aware that a "data exporter" has a due diligence burden when it or its processors are using any mechanism for any restricted transfer, and that we (or our Administrators) will be the "data exporter" in respect of a restricted transfer of Member and Beneficiary Data. The assessments which must be undertaken as part of such due diligence are known as transfer risk assessments. We are aware that the ICO expects us (or our Administrators), as the "data exporter" to check whether the importer (overseas) can in practice comply with transfer mechanisms (for example – though the due diligence obligation is more complex than this). Even where we are not the "data exporter", we will have Members' and Beneficiaries' interests in mind, and will wish to ensure lawful transfers. We will consult with Scheme legal advisers as appropriate.

We will keep a list of all restricted transfers (and mechanisms used for them) in our Data Record.

We will ensure that our Administrators have processes in place to consider data protection whenever a Member or Beneficiary requests an overseas transfer.

5. HOW LONG WE KEEP DATA FOR AND HOW WE DESTROY IT

5.1 Keeping information

We will not keep Member or Beneficiary personal data for longer than is necessary to achieve the purposes set out in Section 1.

For so long as any benefit is payable from the Scheme to or in respect of a Member or Beneficiary, we will retain so much of their personal data as is necessary to ensure that we can pay the benefit correctly.

When a Member or Beneficiary dies or transfers their benefits out of the Scheme, we will continue to hold so much of their personal data as we consider is necessary following such event(s). The reason that we keep a limited but necessary tranche of personal information in such cases is so that we can continue to achieve the purposes in Section 1 and deal with any queries in relation to mistakes or potential underpayments or overpayments for as long as the law requires us to do so. We do not want to be in a position where we are unable to satisfy our legal obligations and/or respond to a query or complaint from a former Member or Beneficiary.

The maximum periods for which we will keep personal data are as follows:

- The majority of the personal data that we hold will be kept for a period of 75 years from the end of the Scheme year in which a transfer out occurs or the last payment of any benefits from the Scheme is made to or in respect of the Member or Beneficiary.

We will keep our record retention periods under review to ensure that we are not keeping personal information for longer than necessary, having regard to the purpose(s) of its processing.

5.2 Destroying information

We will review all the personal data we hold subject to a review being undertaken periodically. If any personal data is no longer needed, we will ensure that it is destroyed.

When we identify data to be destroyed, we will do the following:

- Request all directors of the Trustee to destroy any such data that they hold in relation to relevant Members or Beneficiaries.

- Instruct the Administrators to ensure that any such data they hold in relation to relevant Members or Beneficiaries is destroyed, and then confirm when they have destroyed it.

- Request the Administrators to contact any other parties to whom they have passed or are passing such data to ask for confirmation of destruction.

- Instruct any other parties to whom we have directly passed or are passing such data to destroy it and ask for confirmation of destruction.

5.3 What destruction of data means

Where data is held in a paper format, destruction means that the data will be shredded.

Where data is held in an electronic format, destruction means that the data is put permanently beyond use.

Where data is held by third parties, we will rely on confirmation from them that data has been properly destroyed.

6. RIGHTS IN RELATION TO THE DATA WE HOLD

6.1 Right of access to information we have

Members and Beneficiaries are entitled to be told what information we hold about them and to be given a copy of that information. We are aware of the ICO's statutory code of practice about data subject access requests.

On request, we will also tell Members and Beneficiaries:

- The purpose for which we process their data (as explained in Section 1).

- What type of information we hold about them (as set out in Section 2).

- If we have not collected the information from the Member or Beneficiary themselves, where the information we hold comes from (as set out in Section 3).

- To whom we have disclosed it or intend to disclose it (as set out in Section 4).

- For how long we intend to keep it (as set out in Section 5).

- About their rights in respect of their personal data, including:

- the right to be forgotten in certain circumstances (also known as the right to erasure - see Section 6.3 below);

    - the right to restrict processing (i.e. that the Trustee stops processing) their personal data in certain circumstances, for instance where the Member claims it is inaccurate (until the accuracy is verified); where the processing is unlawful and where they request that our use of it is restricted; or where we no longer need the personal data (see Section 6.4 below);

    - the right to data portability where processing is automated and based on consent or performance of a contract (in such circumstances the Member or Beneficiary has the right to their personal data in a structured machine readable format, and the right to have it transmitted to another data controller);

    - the right to object in certain circumstances to the processing of their personal data (including for direct marketing);

    - their rights relating to automated decision-making about them; and

    - the right to make a complaint to the Information Commissioner's Office.

We will provide this information to Members and Beneficiaries without undue delay, usually within one month of receiving their request.

We will not charge for providing information the first time it is requested. We may make a reasonable charge for subsequent requests if they are manifestly unfounded and/or excessive, based on the administrative cost to us, in accordance with ICO guidance from time to time.

Where the Member or Beneficiary makes an electronic request (for example, by e-mail), we will provide the information in an electronic form (unless the Member or Beneficiary requests otherwise).

6.2 Right to have information corrected or updated

A Member or Beneficiary may ask us to correct any inaccurate personal data that we hold in relation to them "without undue delay". They may also ask us to stop processing their data (in some circumstances including while we check whether it is correct).

Whenever a Member or Beneficiary notifies us (or our Administrators) of a change in the personal information we hold about them, we will instruct our Administrators to ensure that all relevant systems are updated within 1 month of receiving the information. We will also instruct our Administrators to notify all other parties who may be processing the incorrect data on our behalf of the change. This notification should take place within 1 month of receiving the information from you.

Where a Member or Beneficiary notifies us that any information we hold in relation to them is incorrect, we will pass that notification to our Administrators and the Administrators will check the information and correct it (if necessary) in relation to all relevant systems within 1 month. When this has been done, the Administrators should confirm that fact to us within one month of us receiving the request.

We will also instruct our Administrators to take all reasonable steps to pass the corrected information to all other parties who process data on our behalf with a request that they correct the information that they hold and confirm when they have done so.

6.3 Right to be forgotten

A Member or Beneficiary can request erasure of their personal data "without undue delay" where:

- it is no longer needed for the purpose for which it was collected (see Section 1);
- they have withdrawn their consent to processing (if we were relying on that as the basis for lawful processing) and no other legal reason applies to justify the processing;
- they object to the processing and there is no overriding legal reason to continue it;
- the personal data has been unlawfully processed; or
- erasure of the data is required for compliance with another law to which we are subject.

6.4 Right to restrict processing

Members or Beneficiaries can require us to stop processing their personal data when one of the following applies:

- where the Member or Beneficiary is contesting the accuracy of it;
- where the processing is unlawful and the Member or Beneficiary wants us to restrict the use of it instead of erasing it;
- where we no longer need it for the purposes for which it was collected but where the Member or Beneficiary needs the personal data to bring or defend claims in their personal capacity; or
- where the Member or Beneficiary has objected to the processing and where we are considering whether our legitimate interests override those of the Member or Beneficiary.

6.5 Administrative processes for complying with Member/Beneficiary requests

When we receive a request directly from a Member or Beneficiary in relation to one of the rights dealt with in this section, we will pass the request to our Administrators within 5 working days, to be dealt with in accordance with the instructions set out below.

The Administrators will determine whether the Member or Beneficiary has successfully engaged one of the rights set out above. Where they have not, the Administrators will explain in appropriate language to the Member or Beneficiary why the right has not arisen and decline to take further action in relation to the request.

Where a Member or Beneficiary has made a valid request in relation to their data that requires action to be taken, the Administrators will ensure that such action is taken within one month of the request being made. (However, this time period may be extended where requests are complex or numerous and in this case, the Administrators will inform the Member or Beneficiary within one month of the receipt of the request and explain why the extension is necessary.)

We will ask our Administrators to confirm that their staff are appropriately trained to know what rights Members or Beneficiaries have and to recognise requests to exercise such rights and deal with them when they arise.

We will instruct our Administrators to take all reasonable steps to ensure that any valid requests are passed to any other parties who also hold Member or Beneficiary data (as set out in the Data Record) and to seek confirmation that they have acted upon such requests.

We will ensure that Members and Beneficiaries are provided with clear information about what rights they have in relation to their data.

7. HOW WE KEEP INFORMATION SECURE

7.1 Information being handled by the Trustee

Individual directors of the Trustee will ensure that, where they need to be provided with personal data about a Member or Beneficiary:

- All trustees are issued with a company email address and personal email addresses will not be used
- Personal information included in emails will be sent in passworded documents and where possible data will be anonymised.
- Hard copy data will be stored in a secure location.
- All data will be properly destroyed or permanently deleted as soon as it is no longer required, including upon the individual director ceasing to hold office.

Individual directors of the Trustee will be given appropriate training on how to keep data secure and delete or destroy it when required.

7.2 Information being handled by other parties

All agreements that we have with another party who handles Member and Beneficiary data on our behalf will require that party to keep the data securely in accordance with specific requirements of Data Protection Legislation.

When we or our Administrators transfer data to other parties, consideration will be given to whether this data can be anonymised.

7.3 When we transfer data to another party, we will ensure that the transfer is made in a manner that keeps the data secure in accordance with Data Protection Legislation. We will carry out appropriate investigations in relation to anyone to whom we transfer Member or Beneficiary data.

7.4 Information being handled by other parties

With Scheme information now routinely being received, held and transmitted in electronic format, cyber-security is an important issue for the Trustee. We note that phishing and other cyber-security incidents affecting UK organisations (including pension schemes) are increasingly common, and that the Pensions Regulator has issued detailed guidance on this topic.

We are aware of the importance of taking appropriate steps to protect personal data against attacks by cyber-criminals. We are also aware that if cyber-incidents affect the systems of our Administrators or any other processor, as Trustee, we face statutory risk, and that we are expected to find out from our Administrators and other processors what cyber-security measures and staff training against phishing attacks (as a type of cyber-security incident of increasing risk) they implement.

8. WHAT HAPPENS WHERE THINGS GO WRONG

8.1 Where data is lost or destroyed

Where there is a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data (a breach), we will consider as soon as possible what action we need to take.

As a first step, the Chair of the Trustee (currently Leonora Scaife) must be notified immediately.

Within 48 hours of becoming aware of a breach we will consider what we can do to put it right and the likely impact it will have on any Members and Beneficiaries whose data was involved. We will work with service providers where relevant to gather as much information as possible in order to understand the extent of the breach and the steps needed to contain and mitigate the effects of the breach.

Our Administrators and other parties who handle personal data on our behalf are contractually required to notify us as soon as they become aware of a breach and we take all reasonable steps to ensure that they are aware of this requirement.

8.2 Notifying the ICO

Unless we consider that a breach is unlikely to result in a risk to the rights and freedoms of individuals, we will notify the ICO within 72 hours of becoming aware of it and provide the ICO with any information we are required to by law. We will also consider whether a separate notification to the Pensions Regulator is required.

These notifications will be made without undue delay and, where it is not possible to provide all the required information to the ICO at the same time, the information may be provided in phases without undue further delay.

8.3 Notifying Members or Beneficiaries

Where a breach is likely to result in a high risk to the rights and freedoms of Members or Beneficiaries, we will directly notify those whose data is affected, following consultation with relevant stakeholders and legal advisors, where necessary.

Data Protection Legislation provides that we need not notify Members and/or Beneficiaries if any of the following conditions are met:

- We have implemented appropriate technical and organisational protection measures and those measures were applied to the personal data affected by the breach (in particular those that

render the personal data unintelligible to any person who is not authorised to access it, such as encryption).

- We have taken subsequent measures which ensure that the high risk to the rights and freedoms of Members and/or Beneficiaries is no longer likely to materialise.

- Notification would involve disproportionate effort. In such a case, there must instead be a public communication or similar measure, whereby the Members and/or Beneficiaries are informed in an equally effective measure.

- Our notification to affected Members and Beneficiaries will set out the following important information (this may also be subject to ICO guidance):

- The nature of the breach including, where possible the categories and approximate number of individuals concerned and the categories and approximate number of personal data records concerned.

- The name and contact details of someone who can provide more information about the breach.

- An outline of what we believe the likely consequences of the breach are.

- A description of the measures we take to deal with the breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.

These notifications will be made without undue delay.

8.4 Evaluating the response

Following a breach, we will evaluate the effectiveness of the response to the breach and identify any amendments required to this Policy as a result, and /or will suggest adjustments to our or the Administrators' technical or organisational measures in general.

We will maintain a data breach log to record any instances of a data breach along with details of the action taken in relation to the breach.

Appendix 1

Meaning of key terms used in this document

Administrators: means the person(s) or firm(s) who administer the Scheme on behalf of the Trustee. As at the date of this policy, the Administrators are JLT Benefits Solutions of St James's Tower, 7 Charlotte Street, Manchester M1 4DZ.

Beneficiary: means any person who may be entitled to a benefit from the Scheme in relation to a Member.

Controller: means the Trustee and anyone else who (either alone or jointly with others) determines the purposes and means of the processing of personal data.

Data Protection Legislation: means the UK GDPR and, if and to the extent applicable the EU GDPR, together with any legislation and/or regulation implementing or made pursuant to them, or which amends, consolidated, replaces or re-enacts any of the same (including the Data Protection Act 2018) and all other applicable laws relating to the use of personal data and privacy that may exist in the relevant jurisdiction.

Data Record: means the document that sets out what personal data the Trustee holds, why the Trustee needs that data and with whom the data is shared.

EEA: means the European Economic Area (i.e. the EU member countries plus Iceland, Norway and Liechtenstein). As at the date of this policy, the UK is in the EEA since it is part of the European Union.

Information Commissioner's Office / Information Commissioner / ICO: means the UK's data protection authority for the purposes of Data Protection Legislation. It is empowered to take enforcement action in the event of non-compliance with Data Protection Legislation and/or other privacy laws. In addition, it is empowered to issue guidance and codes of practice about this. Its guidance and codes do not have the force of law but it is expected by the ICO that data controllers (including the Trustee) will adhere to them.

General Data Protection Regulation / EU GDPR: means Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. It will apply from 25 May 2018. The GDPR will apply directly in all member states (including, as at the date of this policy, the UK) without the need for any implementing legislation.

Member: means an active, a deferred, pension credit or pensioner member of the Scheme.

Personal data: means information held by the Trustee (or advisers or service providers) from which living Members or Beneficiaries can be identified. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. For instance, employee/member ID numbers do not by themselves reveal names of the Members, but since the Trustee can link those numbers to named individuals, the numbers are personal data.

Processing: means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. In effect, it includes any activity involving personal data.

Processor: means anyone who processes Member or Beneficiary data on behalf of the Trustee for the purposes set out in Section 1. For example, the Trustee may from time to time appoint other persons to act as its data processors in relation to processing which it considers to be inherent in the normal running of the Scheme. These may include (e.g.) IT software providers with maintenance services, or the hosts of the Scheme's servers. The Administrators will carry out certain data processor roles.

Restricted transfer: means a transfer of Personal Data which is undergoing processing or which is intended to be processed after a transfer, to a country or territory to which such transfer is prohibited or subject to any requirement to take additional steps to adequately protect the Personal Data for the transfer to be lawful under the Data Protection Legislation.

Special categories of personal data: means information about a Member or other individual which relates to certain sensitive issues, including their health or sexual orientation/sex life. It also includes information which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data or biometric data for the purpose of uniquely identifying a natural person (i.e. an individual).

Third country: means a country or territory outside the United Kingdom.

UK GDPR: means the UK General Data Protection Regulation (being the EU GDPR (2016/679) as it forms part of domestic law by virtue of section 3 of the European Union (Withdrawal Act) 2018).

Appendix 2
Special Cases

There are some special situations where we may handle data differently from the way we have set out elsewhere in this Policy. This Appendix sets the key circumstances we have identified and what we may do differently in those cases.

1. Part 1 - Sensitive data

8.6 Section 2.4 of this Policy sets out what we will normally do when we need to process special categories of personal data (such as information about health or sexual orientation) and information about criminal convictions and offences (together "sensitive data").

8.7 As we explained in the Policy, sometimes we will seek explicit consent to use sensitive data. On other occasions we will rely on provisions in the Data Protection Act 2018 which allow us to process such data without consent, including where processing is "*necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the data controller or the data subject in connection with employment, social security or social protection*. In addition, the Act also allows us to use sensitive data without explicit consent where there is a reason of substantial public interest.

8.8 To rely on the provisions in the Act which allow us to process sensitive data without consent, we need to have an appropriate policy document in place setting out our approach to various issues. We set out our approach to these issues below.

8.9 Under the Data Protection Legislation we are required to comply with various principles in relation to the personal data we process to ensure that processing is fair. This paragraph provides more information on how we comply with those requirements. Data must be:

8.9.1 **Processed lawfully, fairly and in a transparent manner**: our lawful basis for processing sensitive data is set out in Section 1.2 of this Policy. Except as explained below, we have sent privacy notices to Members explaining what type of information we hold and why and who we might share it with. This is also explained in this Policy.

8.9.2 **Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes**: The reasons we collect personal data are set out in Section 1.1 of this Policy and described in our privacy notices.

8.9.3 **Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed**: The types of personal data we hold are set out in Section 2 of this Policy.

8.9.4 **Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure any personal information that is inaccurate is erased or rectified without delay**: Section 2.5 of this Policy explains how often we will review the personal data we hold to ensure that it remains necessary. Our Administrators are responsible for ensuring that information is accurate and up to date and we have asked them to ensure that they are complying with the requirements of Data Protection Legislation.

8.9.5 **Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed**: Section 5 of this Policy sets out when we will destroy personal data. The same policy applies to sensitive data.

8.9.6 **Processed in a manner that ensures appropriate security of the personal data**: The steps we take to ensure that personal data is kept

secure are set out in Section 7 of this Policy. The same policy applies to sensitive data.

8.10 Our policies in relation to the retention and erasure of sensitive data which we process without consent are the same as our general policies in relation to the retention and erasure of data. These are set out in Section 5 of this Policy. We only keep information as long as we think we need to in order to achieve the purposes set out in Section 1 of this Policy.

8.11 For so long as we retain any sensitive data and for six months after we cease to do so, we will ensure that we:

8.11.1 retain part 1 of this Appendix and the Sections of this Policy referred to in it;

8.11.2 review and (if appropriate) update part 1 of this Appendix from time to time; and

8.11.3 make part 1 of this Appendix and the Sections of this Policy referred to in it available to the Information Commissioner, on request and without charge.

9. Part 2 - Privacy notices

9.1 Normally where we hold personal data about an individual, we will send them a "privacy notice" explaining why we hold that information and what we do with it. However, there are some circumstances where we do not do so, or where we only do so when we subsequently contact the individual for other reasons.

9.2 To protect the rights of individuals in relation to data protection as far as possible, we have assessed how processing personal information without sending out a privacy notices may affect the protection of such information. We have considered the interests of the Scheme in these circumstances and balanced them against the interests of the individual in ensuring that their data is safe and used properly.

Lump sum death benefit nominees

9.3 Where a Member has completed an expression of wish form in relation to lump sum death benefits, that form will contain personal information about the nominee(s). We consider that, having regard to the need for proportionality, it is not appropriate to provide these nominees with a privacy notice for the following reasons:

9.3.1 Lump sum death benefits are provided entirely at our discretion and no one is guaranteed to receive any benefit until we make a decision. In addition, circumstances and nominations may change over time.

9.3.2 We endeavour to minimise the information we hold about nominees and may not have a current address for them.

9.3.3 We do not collect significant amounts of information about nominees on our expression of wish forms and, in our opinion, sending a privacy notice to them would involve a disproportionate effort and could "*render impossible or seriously impair the achievement of the objectives*" of having the information (which is to allow the Trustee to distribute the benefit in accordance with the rules of the Scheme and having regard to the Member's wishes).

9.3.4 Telling nominees that we hold information about them because they have been nominated to receive a benefit which they may not receive could create unrealistic expectations and cause personal difficulties for the Member. It could also potentially become more difficult for a Member to change their nomination if their circumstances changed.

9.3.5 We do not do anything other than store the information until the time comes to consider payment of a death benefit. We request that the expression of wish

form is sent to the Trustee in a sealed envelope which would only be opened in the event of a member's death.

9.3.6 We have a legitimate interest in processing the data contained on a lump sum death benefit nomination form as it is necessary to enable us to discharge our legal responsibilities to pay the correct benefits from the Scheme.

9.3.7 We ensure that any personal data we hold in relation to nominees is held in accordance with the provisions set out in this Policy, including those in relation to security and destruction (retention for no longer than is necessary).

9.3.8 We have not sought the views of any affected individuals on this approach as in our view, and for the reasons set out above, doing so could compromise a Member's confidentiality and would involve disproportionate effort and be impracticable.

Former members

9.4 We may also hold information in relation to former Members who have transferred their benefits out of the Scheme and now have no entitlement to anything from the Scheme ("Former Members").

9.5 We consider that, balancing the interests of Former Members with the interests of the Scheme and the Trustee, it is not appropriate to provide Former Members with a privacy notice:

9.5.1 Although Former Members no longer have any entitlement to benefits from the Scheme, we retain some data in relation to them to allow us and the Administrators to deal with any queries which may arise in relation to past entitlements.

9.5.2 We endeavour to minimise the information we hold about Former Members and may no longer have their current address.

9.5.3 In our opinion, sending a privacy notice to Former Members would involve a disproportionate effort as we would have to obtain additional information about the Former Member to tell them that we retain other information about them.

9.5.4 Balancing the interests of Former Members in being told that we hold minimal data in relation to them against the fact that we would need to acquire additional information in order to do so, and taking into account that they have no rights to any benefit from the Scheme, we consider that it is appropriate not to send them a privacy notice.

9.5.5 We have a legitimate interest in processing the data in relation to Former Members as it is necessary to enable us to ensure that we have correctly discharged our legal responsibilities to pay the correct benefits from the Scheme should questions arise in the future.

9.5.6 We ensure that any personal data we hold in relation to Former Members is held in accordance with the provisions set out in this Policy, including those in relation to security and destruction.

9.5.7 We have not sought the views of any Former Members on this approach as in our view, and for the reasons set out above, doing so would involve disproportionate effort and be impracticable.