

Northumbrian Water Pension Scheme

Data Protection Policy

1 Purpose and scope of this policy

- 1.1 This policy sets out how Northumbrian Water Pension Trustees Limited (the “**Trustee**”) as the trustee of the Northumbrian Water Pension Scheme (the “**Scheme**”) collects and uses personal information about members and former members of the Scheme, their dependants, ex-spouses and beneficiaries, referred to as “**Scheme beneficiaries**” in this policy.
- 1.2 The Trustee is a data controller, as it decides the purpose for collecting this data and how it is processed. It is responsible for this policy and ensuring it is complied with.
- 1.3 This policy applies to the Trustee and its directors. It also applies to employees of Northumbrian Water Limited (the “**Company**”) who provide support to the Scheme, and have access to Scheme personal data. In this policy, these are referred to as the “**Scheme Staff**”.
- 1.4 The Trustee may amend this policy at any time and will carry out a review of its terms at appropriate intervals after it has been adopted. Questions about this policy should be directed to the Secretary to the Trustee.
- 1.5 The Trustee has concluded that it does not need to appoint a data protection officer. If circumstances or requirements change, the Trustee will review this decision.
- 1.6 Terms used in this policy have the meanings ascribed to them by data protection laws applicable to England and Wales unless stated otherwise.
- 1.7 It is noted that, despite Brexit, the Government has confirmed that the GDPR will continue to apply in the UK, as incorporated into UK law by the Data Protection Act 2018.

2 What information does the Trustee collect?

- 2.1 The Trustee has conducted a due diligence exercise to ascertain the personal data held, collected and processed by it and third parties on behalf of the Scheme.
- 2.2 The Trustee maintains a record of processing activities (the “**Data Processing Record**”) which summarises the results of this due diligence and lists the personal data collected by the Trustee and third-party providers on behalf of the Scheme.

Information supporting the Data Processing Record and additional documentation received from third party providers as part of the due diligence exercise is held separately by the Trustee.

- 2.3 Some of the data the Trustee collects falls within “special categories” of personal data, also known as “sensitive personal data”. For example, the Trustee collects information about health for the purposes of assessing the provision of ill-health pension benefits from the Scheme. It also collects information about Scheme beneficiary relationships to provide certain benefits on death and for the purposes of implementing pension sharing orders – this may indicate sexual orientation.
- 2.4 Personal data is collected from Scheme beneficiaries, from the Company, from public bodies such as HMRC and from persons acting as personal representatives. It is collected electronically or in paper files.

3 Complying with the data protection principles

- 3.1 The Trustee is committed to complying with its obligations under data protection laws whenever it, or someone on its behalf, is processing Scheme personal data. As a data controller, there are various data protection principles that the Trustee must comply with. This paragraph sets out the Trustee’s approach to complying with those principles.

Principle 1: lawfulness, fairness and transparency

Lawful basis – personal data generally

- 3.2 The Trustee relies on the following grounds as the lawful basis for processing Scheme personal data:
 - 3.2.1 *Compliance with legal obligations*: to meet trust law duties and responsibilities and/or legislative and regulatory requirements affecting pension schemes.
 - 3.2.2 *Legitimate interests*: the Trustee has a legitimate interest in processing Scheme personal data to ensure the proper management and administration of the Scheme, and to enable benefits to be calculated and paid. The Trustee would also have a legitimate interest in processing Scheme personal data to secure benefits with an insurer in accordance with the Scheme rules, if it decided to do so.

The Trustee has informed Scheme members and, where appropriate, dependents and beneficiaries of their legitimate interests. Although Scheme beneficiaries may object to processing on this ground, the Trustee can override that objection where it has compelling reasons for doing so, such as needing to process personal data to meet its legal obligation to pay benefits.

Lawful basis – special categories of personal data

- 3.3 Additional conditions apply for the Trustee to be able to process special categories of personal data. The Trustee will rely on the following:
 - 3.3.1 the individual giving their explicit consent to the processing;

**Fairness and
transparency**

- 3.3.2 an exemption in the Data Protection Act 2018 allowing the Trustee to process special categories of personal data. In particular, to the extent possible and in cases where obtaining consent is impractical, the Trustee will rely on the exemption that allows data controllers to process special categories of personal data in connection with “employment, social security and social protection” where the processing is necessary for performing or exercising obligations or rights imposed or conferred by law on the data controller or the data subject, and where the Trustee has an appropriate policy document in place. The Trustee considers this policy to be an appropriate policy for the purposes of this exemption. The Trustee acknowledges that, as at the date of this policy, there is a view developing within the pensions industry that this exemption would allow the Trustee to process special categories of personal data without member or beneficiary consent where obtaining consent is impractical and provided the processing is necessary;¹
- 3.3.3 the individual has him/herself made the special category of personal data manifestly public (for example, sexual orientation may be posted on social media);
- 3.3.4 to establish, exercise or defend legal claims.
- 3.4 The Trustee and Scheme Staff will communicate with members (and their dependants and beneficiaries) in a concise, transparent and intelligible manner, using clear and plain language that is easily understood.
- 3.5 The Trustee has provided Scheme members and, where appropriate, dependants and other beneficiaries, with certain specified information required by data protection laws and will update this information from time to time if there are changes to the type of personal data collected or how it is processed.

¹ There is an exemption in the Data Protection Act 2018 which allows data controllers to process special categories of personal data in connection with “employment, social security and social protection” where the processing is necessary for performing or exercising obligations or rights imposed or conferred by law on the data controller or the data subject, and the data controller has an appropriate policy document in place.

As the definition of “social security” in the Data Protection Act 2018 (and connected legislation) is widely drawn and includes sickness, invalidity and old age benefits, a view is developing within the pensions industry that this would allow the Trustee to process special categories of personal data without member or beneficiary consent. We think that the Trustee can reasonably proceed on the basis that the exemption can be used where obtaining consent is impractical and provided the processing is necessary. However, as this is a developing area of the law, we will be monitoring the position going forward.

Where personal data is processed in reliance on the exemption, the Trustee must during the “relevant period” (this period will begin when the Trustee starts processing the personal data in reliance on the exemption and will end 6 months after it ceases such processing):

- retain the appropriate policy document (i.e. this document);
- review and (if appropriate) update it from time to time; and
- make it available to the ICO, on request, without charge.

The Trustee’s Article 30 Processing Record must include information about:

- the exemption being relied on;
- how the processing satisfies Article 6 of the GDPR (i.e. the general legal grounds relied on for processing all Scheme personal data, including special categories of personal data which may fall under the above exemption); and
- whether the personal data is retained and erased in accordance with the Trustee’s policies (forming part of the “appropriate policy”) and, if not, the reasons why.

Principle 2: purpose limitation

- 3.6 Scheme personal data must only be used for the purposes for which it was collected. Put simply, the main purposes for which Scheme personal data is likely to be collected by the Trustee, or other parties on the Trustee's behalf, is to enable the Trustee to properly manage and administer the Scheme, and to calculate and pay benefits.
- 3.7 The Trustee and Scheme Staff should not use Scheme personal data for any purposes which Scheme beneficiaries have not been told about, or which would not be obvious to that individual (or compatible with the original purposes for which it was collected). For example:
 - 3.7.1 The Trustee and Scheme Staff should not access Scheme personal data for their own private purposes, or for friends or family. This is a serious issue and may be a criminal offence for which individuals can be prosecuted.
 - 3.7.2 The Trustee and Scheme Staff should only disclose Scheme personal data with others within their own organisation where that person needs that information to perform their function in line with the specified purposes, or as otherwise permitted by the Trustee.

Principle 3: data minimisation

- 3.8 Essentially, data minimisation means that the Trustee and Scheme Staff must only collect and use personal data needed for the purpose(s) the Trustee has identified (i.e. running the scheme properly, and calculating and paying benefits).
- 3.9 The Trustee and Scheme Staff should continue to collect Scheme personal data needed but will keep data minimisation in mind when asking for information and sharing it, avoiding excess copying and/or sharing of Scheme personal data with others (such as advisers) where it is not strictly necessary.
- 3.10 When reviewing this policy, the Trustee will consider whether there have been any changes in circumstances that necessitate action in relation to minimising the Scheme personal data held. The Trustee will also consider this if it becomes aware of any matter which indicates this principle is not being complied with in relation to Scheme personal data.

Principle 4: data accuracy

- 3.11 High quality personal data is fundamental to providing correct pensions benefits. Members and others are encouraged to inform the administrator of any changes to their circumstances.
- 3.12 The Trustee will update, rectify or erase records, or ask others to do so on its behalf, to the extent required and following such a notification. In some cases, it may be necessary to request evidence to support a change.

3.13 The Trustee and Scheme Staff:

- 3.13.1 must check the accuracy of data when it is collected and at regular intervals that the Trustee decides;
- 3.13.2 should not use personal data they suspect might be out of date without confirming its accuracy;
- 3.13.3 should take every reasonable step to ensure that inaccurate Scheme personal data is corrected or securely deleted without delay. In some cases, however, it may be appropriate to retain out of date personal data if it is the best available and could be used e.g. to help identify the member or as a future starting point for updating purposes; and
- 3.13.4 will update Scheme personal data and relevant databases if they are informed of a change in Scheme personal data.

Principle 5: storage limitation

- 3.14 The Trustee will keep Scheme personal data for as long as is required to meet the purposes for which it was collected.
- 3.15 In practice, this will be the lifetime of the Scheme and for up to 15 years after that time. This is because of the long-term nature of pension schemes, and the possibility of queries, claims and complaints being brought many years after an individual has ceased to be a member or after a scheme has wound up.
- 3.16 When reviewing this policy, the Trustee will consider whether certain types of Scheme personal data are no longer needed, in which case it will generally be destroyed, erased or made inaccessible.

Principle 6: integrity and confidentiality

- 3.17 Scheme personal data must be kept and used securely from when it is first collected until its eventual destruction. The Trustee has in place appropriate technical or organisational measures to protect Scheme personal data against unauthorised or unlawful processing, and against accidental loss, destruction or damage.
- 3.18 The Trustee will impose similar obligations on Scheme Staff and other Scheme providers. The Trustee and Scheme Staff must only transfer Scheme personal data to third parties who have confirmed that they already have appropriate measures in place or who agree to put them in place.
- 3.19 The Trustee and Scheme Staff will observe the following requirements to keep Scheme personal data confidential and secure:

3.19.1 **Access**

Access to Scheme personal data must only be given to those who have a genuine need to access such Scheme personal data to carry out their

duties to the Trustee. Scheme Staff must use secure filing cabinets, access controls and passwords to ensure this.

Appropriate audit trails should be put in place to monitor access and amendments to records (for example, enabling an audit trail to be kept and accessed on computer systems).

Regular checks are undertaken to detect unauthorised or suspicious use of Scheme personal data.

3.19.2 Physical security and storage of documents

Where possible, Scheme Staff and Trustee directors should keep desks clear of all documents containing Scheme personal data at the end of each day. This information must be stored safely and securely in appropriate storage locations (e.g. filing cabinets / drawers / locked offices) and, wherever possible, behind a locked door or drawer with keys kept securely.

Paper documents should be disposed of through confidential waste or by shredding.

3.19.3 Storage of electronic Scheme personal data, off-site working and own devices

All electronic Scheme personal data should be stored on a secure network or on a computer which has appropriate security software installed. The security used on such systems should be regularly updated.

Scheme personal data should never be sent to a personal email unless it is essential that it is sent to all Trustees and where a Trustee only has a personal email or where it is essential to correspond with a potential beneficiary who only has a personal email. Where Scheme personal data is sent to a personal email address, it should be appropriately secured (e.g. with password protection or email encryption).

Trustee directors and Scheme Staff should avoid unnecessary downloading or copying of Scheme personal data.

Where electronic devices are used to process Scheme personal data, Trustee directors and Scheme Staff must do all that is reasonable to keep such devices, associated media and the data contained therein secure at all times.

3.19.4 Printing

When printing Scheme personal data, secure printing areas or locked printers should be used where available. Paperwork containing Scheme personal data should be collected promptly and no unnecessary copies of Scheme personal data should be printed.

4 Transferring personal data

- 4.1 Transfers of Scheme personal data, whether external or internal, must be done securely by Trustee directors and Scheme Staff taking the following steps:
 - 4.1.1 Check information is being sent to the correct recipient.
 - 4.1.2 Where possible, get another authorised individual to check the information before it is sent.
 - 4.1.3 Check the recipient's identity and that they have the authority to receive the data.
 - 4.1.4 Where possible, consider secure methods of transmission, such as password protection or encryption.
 - 4.1.5 Where possible, consider making data anonymous.

5 Who does the Trustee share information with?

- 5.1 The Trustee's Data Processing Record includes details of all third-party providers with whom the Trustee shares Scheme personal data.
- 5.2 In addition to these providers, the Trustee may also transfer personal data to such other third parties whose services the Trustee may require from time to time or where it is under an obligation to do so with regulatory authorities (such as HMRC, the Pensions Ombudsman and the Pensions Regulator).

6 Transferring personal data internationally

- 6.1 The Trustee will only allow Scheme personal data to be transferred out of the European Economic Area (the "EEA") if:
 - 6.1.1 it is transferred at the request and with the consent of the Scheme beneficiary;
 - 6.1.2 it is required to fulfil a contractual obligation in respect of that Scheme beneficiary;
 - 6.1.3 the country to which the data is being transferred is on the Information Commissioner's Office's approved list of jurisdictions ensuring an adequate level of protection;
 - 6.1.4 the data is being sent to an organisation in the United States that is compliant with "Privacy Shield" requirements;
 - 6.1.5 the transfer is being made where "binding corporate rules" are in place to provide appropriate safeguards; or

- 6.1.6 the transfer is governed by a contract put in place with the third party receiving the data containing provisions constituting appropriate safeguards recognised by the ICO.
- 6.2 The Trustee asks its providers to inform it of any transfers of Scheme personal data outside the EEA and of which of the scenarios set out above apply, both on an ongoing basis and as part of its detailed data protection due diligence.
- 6.3 The Trustee will consider whether to take legal advice if Scheme personal data is required to be transferred outside the EEA for a reason other than those detailed at paragraph 6.1 above, or if there is any question as to which of the scenarios set out apply.

7 Data sharing arrangements with third parties

- 7.1 The Trustee may share personal data with third parties in one of three ways which will, in turn, dictate the nature of the agreement that will be entered into with them:

Scenario 1: third party is independent data controller

- 7.2 There are no specific requirements regarding documenting data sharing arrangements between independent data controllers, as each separate data controller is responsible for complying with its data protection responsibilities.
- 7.3 However, in this scenario, the Trustee will seek, where practicable, to enter into an agreement covering, as a minimum, the need for the independent data controller to comply with its obligations and to limit the use and onward transmission of Scheme personal data.
- 7.4 For example, a data sharing agreement is in place between the Trustee and the Company which is the framework under which the Company may request Scheme personal data for a particular project that has a purpose determined by the Company.

Scenario 2: joint data controllers

- 7.5 There are specific requirements applicable to joint data controllers. Where the Trustee acts alongside a joint data controller in relation to Scheme personal data, it will:
 - 7.5.1 determine in a transparent manner how the Trustee and joint data controllers are going to meet their respective responsibilities;
 - 7.5.2 put an arrangement in place to document this in a transparent manner; and
 - 7.5.3 make a summary of this available to members.
- 7.6 As at the date of this policy, the Trustee has not identified any joint data controllers acting alongside the Trustee in relation to Scheme personal data.

Scenario 3: third party is data processor

- 7.7 The Trustee will ensure that all contracts with third parties who are data processors reflect the requirements of data protection laws.
- 7.8 The Trustee will only use third parties as data processors where they provide sufficient guarantees that they have implemented appropriate technical and organisational measures to comply with data protection laws and protect the rights of data subjects.
- 7.9 The Trustee's Data Processing Record sets out the nature of each relationship (as currently understood) between the Trustee and the third parties with whom it shares Scheme personal data and summarises where the contractual arrangements in place with processors have been updated to demonstrate the Trustee's compliance with the above requirements.

8 Individual rights

- 8.1 The Trustee will protect individuals' rights under data protection laws and has informed Scheme members and, where appropriate, dependants and beneficiaries, of these rights.
- 8.2 Requests to see records or exercise these rights should be made in writing to the Secretary to the Trustee. If a Trustee director or other member of Scheme Staff receives such a request, it should be forwarded to the Secretary to the Trustee as soon as possible. The Trustee will respond to requests in exercise of these rights without undue delay and usually within one month² of receipt of the request.
- 8.3 Information will generally be provided free of charge, although the Trustee may charge a reasonable fee in certain circumstances.

9 Accountability

The Trustee is implementing a range of measures to reduce the risk of a breach of personal data:

9.1 Records of processing activity

The Trustee will keep records of all processing activities.

9.2 Privacy by design and by default, and impact assessment

The Trustee is implementing technical and organisational measures to integrate compliance measures into processing activities by ensuring that Trustee directors and Scheme Staff:

² The ICO's guidance now says that the time limit for a response starts from the day the request is received (whether it is a working day or not) until the corresponding calendar date in the next month. Therefore, if a request was received on 27 January 2020, the Trustee should respond by 27 February 2020. If the following month is shorter (and so there is no corresponding calendar date) the date for response is the last day of the following month. And if the corresponding date falls on a weekend or holiday, the deadline falls on the next working day.

- identify privacy risks at the outset of any project or before the implementation of a new project, system or service and plan for them accordingly;
- pseudonymise, encrypt or anonymise Scheme personal data where possible;
- embed privacy into the Trustee's technologies, operations and information architectures and consult all relevant stakeholders;
- maintain the integrity and high standards of products and services; and
- strive to be transparent with individuals about what is done to protect their Scheme personal data.

New products, systems or services developed by parties for the Trustee which will involve processing of Scheme personal data should go through a privacy impact process to determine whether they affect the rights and freedoms of individuals. In some cases where "high risk" processing is identified, a more thorough assessment (a "**Data Protection Impact Assessment**") will be required before it is commenced. This will include a description of the processing activities, the risks arising and measures adopted to mitigate those risks, and, in particular, safeguards and security measures implemented to protect Scheme personal data.

10 Personal data breach

- 10.1 The Trustee will report a data breach to the Information Commissioner's Office without undue delay and, where feasible, within 72 hours of becoming aware of the breach, unless it is unlikely to result in a risk to the rights and freedoms of the individual and the Trustee can demonstrate this.
- 10.2 The Trustee will also need to inform affected individuals where there is a high risk to their rights and freedoms.
- 10.3 The Trustee will keep a register of breaches, in which the Secretary to the Trustee will document any breach, including facts relating to the breach, its effects and the remedial action taken.
- 10.4 In the event that any party processing Scheme personal data becomes aware of a data breach, it has been agreed that they should notify the Secretary to the Trustee and the Trustee Chair (the "**Response Team**"). The Secretary to the Trustee will provide up-to-date contact details of the Response Team to all relevant parties.
- 10.5 As a minimum, the notification to the Response Team shall:
 - describe the nature of the data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of data records concerned;

- communicate the name and contact details of the party's data protection officer or data protection contact;
 - describe the likely consequences of the data breach; and
 - describe the measures taken or proposed to be taken to address the data breach, including, where appropriate, measures to mitigate its possible adverse effects.
- 10.6 The Response Team, or any one or more of their number, will then investigate the breach, taking such professional advice as it deems appropriate, and assess the risk to individuals, as well as establishing whether any action needs to be taken to recover any losses and to limit the damage caused by the breach.
- 10.7 Where appropriate, the ICO will be informed by a member of the Response Team on behalf of the Trustee.
- 10.8 The breach will be recorded in the internal register of breaches and, where applicable, the affected individuals informed.
- 10.9 The Response Team should evaluate the effectiveness of the response to the breach and identify any amendments required to this policy as a result of the Trustee's technical and organisational measures in general, or consider what other action should be taken.

11 Training and guidance

The Trustee and Scheme Staff will receive appropriate training on data protection laws, security requirements and the contents of this policy, both when initially appointed or engaged and on an ongoing basis.

12 Audit

The Trustee will undertake internal audits of their processing activities from time to time. The Trustee, Scheme Staff and (where relevant) third parties must cooperate with these audits.

Approved and adopted by the Trustee on 4 December 2019