

# Data Protection Policy (the “Policy”)

## 1 Who we are

The Electricity North West (ESPS) Pensions Trustees Limited is the trustee (“the **Trustee**”) of the Electricity North West Group of Electricity Supply Pension Scheme (“the **Group**”).

As the Trustee of the Group, we collect and use certain personal information (known as Personal Data) about Group members and, where applicable, their dependants and beneficiaries. Individuals have specific rights when Personal Data about them is collected and used.

For legal purposes, the Trustee of the Electricity North West Group of the ESPS is the Data Controller in respect of your personal information for the purposes of applicable data protection legislation, as we decide the purposes for and the means by which the Personal Data we collect is Processed.

## 2 Purpose of this Policy

Data Protection Legislation places obligations on organisations involved in the Processing of Personal Data about individuals. Both complying with the legislation, and being able to demonstrate compliance, are essential. Protecting Group Personal Data also plays an essential role in ensuring the good governance of the Group more generally.

This Policy sets out how we meet our obligations under Data Protection Legislation. The requirements of this Policy are supplemented by the Privacy Notice available at <https://www.enwlpensions.co.uk/support/privacy-and-data-protection> to which all members have access.

There are substantial fines and other sanctions which can be imposed on organisations for non-compliance with Data Protection Legislation (including a failure to demonstrate compliance with the principles). Organisations can also be liable to pay compensation to individuals for any damage caused by a breach. In addition, a Personal Data Breach may also result in bad publicity and loss of reputation for both the Group and the sponsoring employer.

For ease of reference, key terms used in this Policy are defined in section 5.

## 3 Scope of this Policy

This Policy applies to the Trustee and all persons appointed as directors, officers or managers of the Trustee, the pensions manager, and the secretary to the Trustee, together with all other employees of the sponsoring employer who provide support to the Group and have access to Group Personal Data (collectively referred to as the “Relevant Parties”).

All Group Personal Data collected by us electronically or in structured paper files (or which is intended to be in such a filing system) is covered by this Policy. This Policy sets out the Trustee’s requirements relating to data protection and the legal conditions that must be satisfied in relation to the Processing of Group Personal Data. However, this Policy is also subject to the general requirements of Data Protection Legislation.

Failure to comply with this Policy may mean that Relevant Parties are directly liable for penalties and compensation under Data Protection Legislation and unauthorised use, for private purposes, of Group Personal Data obtained by Relevant Parties may even be a criminal offence in certain circumstances. Failure to comply with this Policy may also mean that Relevant Parties are in breach of their contractual commitments in respect of the Group.

## 4 Responsibility for this Policy

The Trustee is responsible for ensuring that this Policy meets all applicable legal requirements and that all Relevant Parties comply with it. Any questions, exceptions to or breaches of this Policy should be referred to Colin Ross, Group Pensions Manager.

Having considered the requirements of Data Protection Legislation, as well as the advice received from our legal advisers (Sackers & Partners LLP) in February 2018, we have concluded that we do not need to appoint a Data Protection Officer. If our circumstances or regulatory requirements change, we will review this decision with our legal advisers.

## 5 Meaning of key words / phrases used in this Policy

This Policy uses the following key words and phrases:

- **Dashboards Regulations** means the Pensions Dashboards Regulations 2022 (SI 2022/1220).
- **Data Controller** means any legal or natural person who alone, or jointly with others, determines the purposes for and the means by which Personal Data is Processed. For the purposes of this Policy, the Trustee is considered the Data Controller.
- **Data Processor** means any legal or natural person that Processes Personal Data on behalf of the Data Controller, for example, the Group administrators.
- **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, consolidates, replaces or re-enacts any of the same (including the DPA 2018), and all other applicable laws relating to the processing of Personal Data and privacy where relevant.
- **Data Subjects** are individuals on whom Personal Data is held and, in the context of an occupational pension scheme, will include Group members (both current and former), their dependants and beneficiaries (both actual and potential).
- **DPA 2018** means the Data Protection Act 2018.
- **EU GDPR** means the General Data Protection Regulation (EU 2016/679).
- **Group Personal Data** means any Personal Data (including Special Categories of Personal Data) held:
  - in relation to members (both current and former), their dependants and beneficiaries (both actual and potential), including their names, postal addresses, email addresses, dates of birth, national insurance numbers, bank account and salary details, length of pensionable service, pension contributions, pension benefits and “pension identifiers”
  - in relation to individuals who are the subject of a “find request” received by the Group, including names, postal addresses, email addresses, dates of birth and national insurance numbers

- by the Trustee (or on our behalf) about those providing services and advice to the Group (e.g. contacts at the employer, our Group administrators, suppliers and advisers)
- ICO means the Information Commissioner's Office, the UK regulatory body charged with ensuring compliance with Data Protection Legislation.
- **Personal Data** means any information (whether opinion or facts) relating to an identified or identifiable living person (or Data Subject). An identifiable living person is one who can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to his/her identity. The fact that information is publicly available (e.g. on LinkedIn) does not stop Data Protection Legislation applying to it.
- **Personal Data Breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Group Personal Data.
- **Process / Processes / Processing / Processed** covers virtually anything done with Personal Data, including collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination (or otherwise making available), or destruction.

Relevant Parties will almost certainly process some Group Personal Data. The extent of that Processing will depend on the role of the Relevant Parties and the services and/or advice they are asked to provide.

- Relevant Parties has the meaning set out in section 3.
- **Special Categories of Personal Data (i.e. sensitive Personal Data)** is Group Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the Processing of genetic data, biometric data for the purpose of uniquely identifying an individual, data concerning health or data concerning an individual's sex life or sexual orientation.
- For pension schemes, Special Categories of Personal Data are most likely to be relevant when dealing with ill-health, divorce and death cases.
- **Third Parties** has the meaning set out in section 9.
- **UK GDPR** means the EU GDPR as it forms part of domestic law by virtue of section 3 of the European Union (Withdrawal) Act 2018.

## 6 Complying with the Data Protection Principles

We are committed to complying with our obligations under Data Protection Legislation whenever we, or someone acting on our behalf, are Processing Group Personal Data. As Data Controllers, we must comply with the data protection principles set out below.

### 6.1 Lawfulness, fairness and transparency – Personal Data should be Processed lawfully, fairly and in a transparent manner

#### 6.1.1 Lawful basis

We can only process Group Personal Data where we have a lawful basis (or grounds) for doing so under Data Protection Legislation, and we must keep records of what that is or they are. The grounds for Processing which we rely on differ depending on the type of Group Personal Data, namely, whether it is general Group Personal Data (i.e. non-sensitive Personal Data) or Special Categories of Personal Data.

As we must have valid grounds for Processing Group Personal Data at all times, and these grounds may change or cease to exist over time, we will keep the reasons outlined below under review.

### *General Group Personal Data*

The legal grounds for Processing which we generally rely on are:

- *Compliance with legal obligations* – to meet our trust law duties and responsibilities and/or legislative and regulatory requirements affecting pension schemes. This extends to our duties under the Dashboards Regulations, including “matching”, where we use personal data that a user has inputted into a dashboard to search the Group records to check whether that user is a member of the Group, and where we collect further personal data from that user in the event of a “possible match”.
- *Legitimate interests* – as the Trustee, we have a legitimate interest in Processing Group Personal Data to ensure the proper administration of the Group, and to enable us (and relevant Third Parties) to calculate and pay benefits. We also have a legitimate interest in Processing Group Personal Data to secure benefits with an insurer in accordance with the Group rules.

As required under the Data Protection Legislation, we have informed members of our legitimate interests. Although members have the right to object to Processing on these grounds (see section 11), we can override that objection where there are compelling reasons (e.g. because we need to process that Group Personal Data in order to meet our legal obligation to pay benefits).

### **Special categories of Personal Data**

Data Protection Legislation generally prohibits the Processing of Special Categories of Personal Data unless certain conditions are met. The most relevant conditions for us to rely on are as follows:

- the member, dependant or beneficiary having given their explicit consent to the Processing for one or more specific purposes. We will generally rely on consent when Processing Special Categories of Personal Data
- the individual has him/herself made the Special Categories of Personal Data manifestly public
- in order to establish, exercise or defend legal claims, and
- where applicable, the employment, social security and social protection condition for Processing Special Categories of Personal Data.

### **The employment, social security and social protection condition**

Where obtaining explicit consent from the member (dependant or beneficiary) for Processing their Special Categories of Personal Data is not reasonably practicable or may cut across the Trustee’s duties to ensure the proper administration of the Group, the Trustee will rely on the employment, social security and social protection condition for Processing Special Categories of Personal Data set out in Article 9(2)(b) of the UK GDPR (and Article 9(2)(b) of the EU GDPR if and to the extent applicable) and Schedule 1 to the Data Protection Act 2018. This condition 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 the purposes of 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 when the Processing is carried out.

The Trustee considers this Policy to be an appropriate policy for the purposes of this condition. The Trustee confirms it has considered the following in relation to its Processing of Special Categories of Personal Data under this Policy:

- its compliance with the data protection principles (as described in this section 6)
- its retention and deletion policies (section 6.5), and
- the retention period for Group Personal Data (section 6.5).

### 6.1.2 Fairness and transparency

To satisfy the requirement to be fair and transparent, we / Relevant Parties must communicate with members (and their dependants and beneficiaries) in a concise, transparent and intelligible manner, using clear and plain language that is easily understood.

We must tell members (and their dependants and beneficiaries) what Group Personal Data is collected about them, how we intend to use it, who we share it with, if we intend to transfer it to another country outside of the European Economic Area (“EEA”), as well as letting them know how they can contact us with questions or in order to exercise their rights (see section 11). Where Group Personal Data is being transferred outside of the UK or EEA (or to an international organisation), this includes letting members know what safeguards have been put in place, as well as providing details as to who to contact if they wish to obtain a copy or where copies of such safeguards are made available (see also section 8).

We provide our Group members, their dependants and beneficiaries and any dashboard user who contacts the Group to resolve a “possible match” with access to this information in our Privacy Notice available at <https://www.enwlpensions.co.uk/support/privacy-and-data-protection>

If we need to ask for more Group Personal Data or change how Group Personal Data is Processed, we will consider if further information needs to be given to members (their dependants and beneficiaries). We will pay particular attention to providing information about the use of Group Personal Data in a way which the individual would not expect.

References to “dependants and beneficiaries” in this section 6.1.2 means those dependants and beneficiaries of members who:

- are in receipt of a survivor’s pension from the Group, or
- provide Personal Data directly to the Group to allow the Group to pay benefits (eg a death benefit lump sum).

We will not take proactive steps to provide a copy of the Privacy Notice directly to those persons named on the Group’s expression of wish forms, or to users of dashboards where they (i) do not contact the Group in the event of a “possible match”, or (ii) are not a Group member. However, the Group’s Privacy Notice is publicly available on the Group’s website and, in respect of those named on expression of wish forms, members can refer those individuals to that website, should they wish.

## **6.2 Purpose limitation – Personal Data should be collected for specified, explicit and legitimate purposes, and not further processed in a way that is incompatible with those purposes**

Group Personal Data must only be used for the purposes for which it was collected. Put simply, the main purposes for which Group Personal Data is likely to be collected by the Trustee and Relevant Parties on our behalf is to enable us to properly administer the Group, and to calculate and pay benefits. Another key purpose of Processing Group Personal Data is to comply with the Trustees' legal obligations under the Dashboards Regulations.

Relevant Parties should not use Group Personal Data for any purposes which we have not told the members and their dependants and other beneficiaries about, or which would not be obvious to that individual (or compatible with the original purposes for which it was collected). For example:

- Relevant Parties should not access Group 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;
- Relevant Parties should only disclose Group Personal Data with others within their own organisation where that person needs that information in order to perform their function in line with the specified purposes, or as otherwise permitted by us.

In determining whether a new purpose of Processing is compatible with the original purposes, we / Relevant Parties will need to consider any link between the purposes, the context in which the Group Personal Data has been collected, the nature of the Group Personal Data, the possible consequences of the future Processing and any proposed safeguards.

## **6.3 Data minimisation – Personal Data should be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed**

Essentially, data minimisation means that we / Relevant Parties (and Third Parties) must only collect and use the Personal Data needed for the purpose(s) we have identified (i.e. running the scheme properly, and calculating and paying benefits and complying with the Dashboards Regulations). We / Relevant Parties should continue to collect the Group Personal Data we need but should keep data minimisation in mind when asking for information and sharing it, avoiding excess copying and/or sharing of Group Personal Data with others (such as advisers) where it is not strictly necessary.

We shall make regular checks on the relevance of Group Personal Data being collected by Relevant Parties and/or Third Parties to ensure it continues to be proportionate to the purpose.

## **6.4 Accuracy – Personal Data should be accurate and, where necessary, kept up-to-date**

High quality Group Personal Data is fundamental to providing pensions benefits and meeting the Trustees' legal obligations under the Dashboards Regulations. We encourage members, their dependants and beneficiaries to inform Broadstone of any changes to their Group Personal Data and have included their contact details in the Privacy Notice. We will update, rectify or erase records (or ask that other Relevant Parties and Third Parties make the appropriate changes) to the extent required. In some cases, it may be necessary to request evidence to support a requested change.

Broadstone maintain member records which consist of up-to-date and accurate information and are updated and reconciled regularly.

Broadstone receive regular updates on member personal data from us, the Trustee. In support of this, Broadstone carry out a series of regular data integrity checks, including:

- Validation checks and authorisation when creating new member records and making member data changes;
- Data quality checks in line with Pensions Regulator guidance on measuring member data ('common data' requirements);
- Member movement reconciliations;
- UK pensioner existence checks using an external tracing bureau; and
- Overseas pensioner, child dependant and incapacity pensioner existence checks.

Any data discrepancies identified during these reviews are investigated. A standard protocol is followed with an established communication timeframe for the member to respond before payments are suspended until satisfactory documentation is received.

We are able to update member data using a number of different methods. Standard interface files are available and can be imported into the administration system following validation checks. Members can also update their own data using a secure member website which requires a unique user log-in and password authentication.

Broadstone may also engage a Third Party on the Trustee's behalf to verify a member's, dependant's or beneficiary's identity using online electronic identity verification if the individual agrees to this. The circumstances in which online electronic identity verification might be used include:

- verification prior to initial payment of pension, death benefit payments or transfers out;
- change of address requests;
- new addresses added to member records when they have previously been missing from records;  
or
- requests to change bank account details.

All communication requires authorisation from the Trustee / the member before amending member data. Member correspondence is scanned onto a document management system and filed with the member record for reference.

Benefits statements are provided to active members annually which gives the opportunity to review personal data and raise queries with the Broadstone Administration team.

#### **6.5 Storage limitation – Personal Data should be kept in a form which allows an individual's identification for no longer than is necessary for the purposes for which the Personal Data is processed**

Group Personal Data shall not be kept for longer than is required in order to meet the lawful purpose(s) for which it was collected. Where there is a statutory (or other legal) maximum limit on how long we can retain certain Group Personal Data for, we will comply with that restriction.

To meet the requirements of both UK tax and pensions law, we must keep certain Group Personal Data for a minimum of 6 years. However, given the long-term nature of pension schemes, and the possibility of claims being brought in relation to the Group many years after an individual has ceased to be a member, we consider that it is necessary to keep Group Personal Data for so long as the member is entitled to

benefits under the Group and for an appropriate period after that time, which reflects the potential for queries and complaints.

We will review Group Personal Data on a regular basis. If we conclude that certain Group Personal Data is no longer needed, that Group Personal Data will generally be destroyed. We will also ensure that Relevant Parties and Third Parties regularly review Group Personal Data held on our behalf and that appropriate steps are taken to delete, destroy or prevent access to Group Personal Data that is no longer required. All such actions will be undertaken securely.

#### **6.6 Integrity and confidentiality – Personal Data should be processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful Processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures**

Group Personal Data needs to be kept and used securely from when it is first collected until its eventual destruction. We therefore need to put in place appropriate technical or organisational measures to protect Group Personal Data against unauthorised or unlawful Processing, and against accidental loss, destruction or damage, and to ensure that Relevant Parties and Third Parties do likewise. We will only transfer Group Personal Data to Third Parties who have confirmed that they already have appropriate measures in place or who agree to put them in place.

The requirement to keep Group Personal Data confidential and safe applies however information is held, whether on laptops or other portable devices, desktops, disks, USB sticks, as part of a database, in paper form or otherwise.

All Relevant Parties and Third Parties must observe the following requirements to keep Group Personal Data confidential and secure:

##### **6.6.1 Access**

- Access to Group Personal Data must only be given to Relevant Parties and Third Parties who have a genuine need to access such Group Personal Data to carry out their duties to us. Relevant Parties and Third Parties 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). This is important to ensure that there is accountability for Group Personal Data.
- Ensure that regular checks are undertaken to detect unauthorised or suspicious use of Group Personal Data.

##### **6.6.2 Physical security and storage of documents**

- Where possible, Relevant Parties and Third Parties should keep desks clear of all documents containing Group 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).
- Wherever possible, doors to areas where Group Personal Data is stored and filing cabinets which contain Group Personal Data should be locked and keys kept securely.
- Paper documents should be disposed of through confidential waste or by shredding.

### 6.6.3 Storage of electronic Group Personal Data, off-site working and own devices

- All electronic Group 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.
- Group Personal Data should never be sent to a personal email, apart from individual trustee email addresses when required to make discretionary decisions relating to ill-health, divorce and death cases; sending paperwork relating to internal dispute resolution procedures and sending trustee minutes for approval.
- Unless we agree otherwise, or it is required in order to provide services to us, Relevant Parties and Third Parties should avoid unnecessary downloading or copying of Special Categories of Personal Data or large volumes of Personal Data. This applies to downloading or copying locally onto a database or any other device including laptops, desktops, mobile phones or other portable devices, USB sticks, CD-ROMs, databases, in paper form or otherwise
- Relevant Parties and Third Parties who use electronic devices to process Group Personal Data must do all that is reasonable to keep such devices, associated media and the Group Personal Data contained therein secure at all times.

Group Personal Data held on USB sticks, CD-ROMs, floppy disks, or similar should be deleted when no longer required or, alternatively, such media should be physically destroyed.

### 6.6.4 Printing

- When printing Group Personal Data, secure printing areas or locked printers should be used where available. Paperwork containing Group Personal Data should be collected promptly and no unnecessary copies of Group Personal Data should be printed. Where available, printer settings should be checked to ensure that the correct number of sheets has been printed.

## 7 Transferring Group Personal Data

Any transfers of Group Personal Data must be done securely, whether externally to Third Parties such as employers or Group administrators, or internally within the Trustee body / between Relevant Parties.

Before transferring Group Personal Data (whether by email, post, fax or otherwise) whether internally or externally, Relevant Parties and Third Parties:

- must check that the information is being sent to the correct recipient
- should consider asking another individual (namely, someone else who is authorised to have access to the Group Personal Data) to check documents before they are sent. In particular, such checks should ideally be carried out when transferring Special Categories of Personal Data or large volumes of Group Personal Data
- where required, should check the recipient's identity and/or that they have the authority to receive Group Personal Data. This may involve carrying out checks to verify their identity, particularly if information is being released over the phone
- should consider using secure methods of transmission, including password protection, encryption and "pseudonymisation" (i.e. making Group Personal Data available on the basis that it can no

longer be attributed to a specific individual without the use of additional information which is kept separately)

- where possible, should consider completely anonymising Group Personal Data.

Email encryption should be used when large volumes of Group Personal Data are sent by email (e.g. transfers of large spreadsheets of Group Personal Data) or where Group Personal Data that might be considered sensitive or confidential is sent by email.

## 8 International transfers

Data Protection Legislation restricts transfers of Personal Data outside of the UK or EEA, unless there is adequate protection for the Personal Data or prescribed steps have been taken to ensure that the Personal Data is protected.

We do not allow Group Personal Data to be transferred outside of the UK or EEA unless:

- it is transferred at the request and with the consent of the Group member in relation to his/her own benefits (or a dependant or beneficiary, as appropriate)
- it is required to fulfil a contractual obligation in respect of the member (or a dependant or beneficiary, as appropriate)
- there are regulations in place under Article 45A of the UK GDPR approving transfers to that country or territory or, where relevant, a finding of adequacy pursuant to Article 45 of the EU GDPR
- the country to which Scheme Personal Data is being transferred is on the ICO's approved list
- the Group Personal Data is being sent to an organisation based in the United States which is compliant with "Privacy Shield" requirements, or
- a contract has been put in place with the third party/parties to which the Group Personal Data will be transferred containing appropriate safeguards in relation to the Group Personal Data, and we consider that the protection for the Data Subject's Personal Data would not be "materially lower" after the transfer.

Relevant Parties and Third Parties must inform us of any Processing of Group Personal Data outside of the UK or EEA and they should also seek legal advice if:

- they or someone acting on their behalf will Process / are Processing Group Personal Data outside of the UK or EEA (including where the third party is based outside the UK or EEA or the Group Personal Data will be held or remotely accessed by a third party or its sub-contractors in a location outside of the EEA); or
- there are questions about what Group Personal Data may be transferred outside the UK or EEA.

Safeguards being relied on where international transfers are made include:

- reliance on an adequacy regulation, the UK will recognise the adequacy decisions made by the Commission existing as at 31 December 2020. As at 31 December 2020, the EU Commission has determined that the following countries offer adequate protection for data transfers: Andorra, Argentina, Canada (commercial organisations), Faeroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland and Uruguay

- the International Data Transfer Agreement issued by the ICO
- when the individual has explicitly consented to the transfer
- when it is necessary to perform a contract
- when it is necessary for important reasons of public interest, or
- when it is necessary for the establishment, exercise or defence of legal claims.

## 9 The Third Parties we share Group Personal Data with

As Trustee, we need to share Group Personal Data with various Third Parties in order to help us to properly administer the Group or, where relevant, because certain Third Parties have a justifiable interest in receiving Group Personal Data. We are also under an obligation to share Group Personal Data with certain regulatory authorities, such as HM Revenue & Customs and other statutory bodies (e.g. the Pensions Ombudsman and the Pensions Regulator). We can be fined and subject to other action if we fail to provide certain information to these authorities

We share Group Personal Data with the following (which are referred to collectively in this Policy as “Third Parties”):

- the pensions manager, together with all other employees of the sponsoring employer who provide support to the Group and have access to Group Personal Data
- the sponsoring employer and other entities in the sponsoring employer’s group
- the Group’s professional advisers, including the Group actuary, auditor, investment adviser, benefit consultant, medical advisers, and lawyers
- our Group administrators, who are responsible for the day-to-day administration of the Group on our behalf
- the providers of software and/or services to the Scheme administrators from time to time for the purpose of undertaking electronic identity verification
- the advisers and printers who help us prepare various communications we send to members, such as the annual benefit statement
- third parties that form part of the “dashboard ecosystem” and the Group’s Integrated Service Provider (ISP), which provides a service allowing pensions information from the Group to be connected to that ecosystem
- our appointed insurance company or companies for the purposes of life insurance, group income protection and additional voluntary contributions
- depending upon how we pay pensions, organisations to whom we send Group Personal Data in order to effect a BACS transfer (the Bankers' Automated Clearing Service) or CHAPS (the Clearing House Automated Payment System) in the UK and/or a payment via Global Disbursements at HSBC, the Group administrators’ banking providers, when pensions are being paid overseas
- our financial adviser appointed for at retirement support and advice
- the service provider for the online board meeting portal

- the election services provider
- the mortality and address tracing agencies
- central and local government ombudsmen and regulatory authorities
- such other Third Parties whose services we may require from time to time.
- insurers or re-insurers providing services for the purpose of liability and risk management exercises.

## 10 Data sharing arrangements with Third Parties

Under Data Protection Legislation, the obligations that Third Parties are required to comply with (and the terms that need to be included in contracts) will depend upon whether they handle Personal Data as a Data Controller or a Data Processor. The distinction is important in determining who is primarily responsible for complying with legal requirements, and who can be liable for fines and compensation.

We may share Group Personal Data with Third Parties in one of three ways, which will, in turn, dictate the nature of the agreement which will need to be entered between us.

### 10.1 Data Controller to independent Data Controller

Third Parties providing services to the Group will be an independent Data Controller where they use the Group Personal Data for purposes which are different to our own. Examples of this type of relationship will include when we share Group Personal Data with the employer and the Group actuary. Also, organisations or individuals under certain legal obligations to hold Personal Data, for example, accountants and insurers, might also be independent Data Controllers of Group Personal Data. Also, the Money and Pensions Service, in its capacity as running the central digital architecture that underlies the dashboards ecosystem.

Owing to the nature of their role, the Group actuary will be a Data Controller of Group Personal Data alongside the Trustee and they are required to give you details of how they treat your information. A summary is appended to the Privacy Notice available at <https://www.enwlpensions.co.uk/support/privacy-and-data-protection>

The Group's legal advisers, Sackers & Partners LLP, (in certain circumstance) are also data controllers in relation to your personal data. For more information about what personal data they hold about you and how they use it see their [privacy notice for pension scheme members, beneficiaries and client's employees](#).

The sponsoring employer is also a joint Data Controller of Group Personal Data with us. Their privacy policy can be found at <https://www.enwl.co.uk/misc/privacy-policy/>

There are no specific requirements under Data Protection Legislation regarding documenting data sharing arrangements between independent Data Controllers, as each separate Data Controller is responsible for complying with relevant requirements. However, when sharing Group Personal Data with an independent Data Controller we will enter into an arrangement covering, as a minimum, the need for the independent Data Controller to comply with its obligations under Data Protection Legislation and, to the extent appropriate, limiting the use and onward transmission of Group Personal Data.

## 10.2 Joint Data Controllers

Where two or more parties jointly determine the purposes and means of Processing Personal Data (using the same Personal Data for the same purposes), they will be joint Data Controllers. Each joint Data Controller has full liability resulting from a Personal Data Breach, unless one of the joint Data Controllers can show that it is not in any way responsible.

From 25 May 2018, Data Protection Legislation sets out specific requirements in relation to joint Data Controllers. Where we act alongside a joint Data Controller in relation to Group Personal Data, we will do the following as a minimum:

- determine, in a transparent manner, how we are going to meet our respective responsibilities for complying with Data Protection Legislation, including meeting the information requirements to individuals (e.g. by a joint privacy notice) and dealing with individuals' rights (see section 11 below)
- put an arrangement in place to document the above
- make a summary of that arrangement available to members.

## 10.3 Data Controller to Data Processor

This is the most common arrangement that we enter with Third Parties. Our Data Processors include our Group administrators, pensions manager, insurance companies, insurance providers, annuity broker, financial adviser, medical advisers, printers, legal advisers, benefit consultants, investment advisers, auditors, the service provider for the online board meeting portal, the election service provider, the service provider for electronic identity verification, central and local government ombudsmen and regulatory authorities, and mortality and address tracing agencies. Dashboard ISPs and our legal advisers might also be Data Processors, depending on the circumstances

Under Data Protection Legislation, there must be a binding contract in place between a Data Controller and a Data Processor covering certain minimum requirements. We will ensure that all contracts with Third Parties who are Data Processors reflect the requirements under Data Protection Legislation, including that the Data Processor must:

- act only on our written instructions, unless otherwise required by law
- ensure that persons authorised to process Group Personal Data are obliged to keep it confidential
- implement appropriate measures to ensure the security of Processing
- assist us in meeting our security obligations under Data Protection Legislation, as well as in notifying breaches and carrying out a data protection impact assessment (if required)
- assist us in dealing with members' rights, for example, a Data Subject access request
- subject to our choice, delete or return all Group Personal Data to us at the end of the contract where possible
- engage a sub-processor only with our prior written agreement and having imposed similar contractual requirements on the sub-processor (and acknowledging that the Data Processor will remain fully liable to us for any breach by the sub-processor)

- make all information needed to demonstrate compliance with relevant obligations of Data Protection Legislation available to us
- allow for, and contribute to, audits carried out by us or someone else on our behalf.

In addition, we will only use Third Parties as Data Processors where they provide sufficient guarantees that they have implemented appropriate technical and organisational measures so that the Processing of Group Personal Data by them meets the requirements of Data Protection Legislation and the protection of individuals' rights.

## 11 Individuals' rights

We will always protect individuals' rights under Data Protection Legislation (to the extent applicable) including:

- **Right to information** – we make information available to our Group members, their dependants and beneficiaries about how Group Personal Data is Processed in our Privacy Notice (see section 2 above). This includes details of their various rights outlined in this section
- **Rights of access (also known as a “Data Subject access request”)** - Data Subjects have the right to see Group Personal Data that is held about them and a right to have a copy provided to them, or someone else on their behalf, in a machine readable (namely, digital) format. The Data Subject is only entitled to information that we are able to provide based on a “reasonable and proportionate” search.
- **Right to rectification** – if at any point a Data Subject believes that the Group Personal Data we hold about them is inaccurate, they can ask to have it corrected
- **Right to restrict Processing** – Data Subjects can require us to limit the Processing of their Group Personal Data in certain circumstances, for example, whilst a complaint about its accuracy is being resolved
- **Right to be forgotten (or to erasure)** – Data Subjects can request that their Group Personal Data is deleted altogether, although the Trustee can override this request in certain circumstances
- **Right to object to Processing** – where we are relying on legitimate interests as a reason for Processing, Data Subjects can object to having their Group Personal Data Processed, although we can override this objection and continue Processing that individual's Group Personal Data where this is justified.
- **Withdrawing consent** – where we have relied on a Data Subject's consent to Process their Group Personal Data (for example, where a member has provided medical information to us as part of an early retirement application on grounds of ill-health), he/she can withdraw that consent at any time by notifying us. However, withdrawing consent will not affect the Processing of any Group Personal Data which took place beforehand and it may be possible for us to continue Processing that individual's Group Personal Data where this is justified.
- **Automated decisions** – a Data Subject also has a right not to be subject to the use of entirely automated decisions (including profiling linked to direct marketing) which produce legal effects or significantly affect the individuals. We do not use either of these in relation to Group Personal Data and neither do any Third Parties, apart from in relation to electronic identity verification in certain circumstances (including verification prior to initial payment of pension, death benefit

payments or transfers out; change of address requests; new addresses added to member records when they have previously been missing from records; and requests to change bank account details).

- **Transfers outside of the UK or EEA** – where Group Personal Data is being transferred outside of the UK or EEA (or to an international organisation), we will tell members about the safeguards put in place, as well as providing details as to who to contact if they wish to obtain a copy or where copies of such safeguards are made available.

### How we meet those rights

We will provide any required information or communication relating to the Processing of Group Personal Data to a Data Subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language. We inform Data Subjects of the above rights in the Privacy Notice.

We will respond to requests without undue delay, and usually within one month of the later of the receipt of the request, the receipt of any additional information necessary to confirm the Data Subject's identity (where we have reasonable doubts over their identity) or the payment of any fee charged (where relevant). We may pause this clock to ask for clarification of the request, and we may extend the usual one month period by two further months, where this is necessary due to the complexity and/or number of requests from the Data Subject.

Information will generally be provided to Data Subjects free of charge, although we can charge a reasonable fee in certain circumstances.

Requests by Data Subjects to see their records or to exercise any of their other rights under Data Protection Legislation should be made, in writing, to the Group Pensions Manager, Colin Ross, who will take appropriate steps to deal with the issues raised.

Relevant Parties must:

- take care when entering information in free-text areas in any software systems as individuals to whom the information refers (such as Group members) may see it at a later date. Information should only be entered which is appropriate and justifiable
- forward any requests to see Group Personal Data from any Data Subjects, or any other requests or complaints relating to the way in which their Group Personal Data is processed, to Colin Ross, Group Pensions Manager, immediately. There are often strict timescales for complying with such requests, so requests must be forwarded as soon as possible following receipt.

### Right to complain

From 19 June 2026 a Data Subject may make a complaint to the Trustee (as the Data Controller) if they consider that there has been an infringement of the Data Protection Legislation in respect of their Personal Data.

The Trustee has a process for handling data protection complaints, which is set out in a separate data protection complaints process [include link[EL4.1]].

## 12 Accountability

Data Protection Legislation requires us to implement a wide range of measures to reduce the risk of a Personal Data Breach occurring and to demonstrate that we are taking data governance seriously. A description of some of the measures we have put in place to meet this requirement are set out below.

### 12.1 Records of Processing Activity

All organisations are required to keep records of all Processing activities, whether acting as a Data Controller or a Data Processor.

As Data Controllers, under Article 30, the Trustee will need to keep written records of:

- their name and contact details and, where applicable, any joint Data Controller, and the Data Controller's representative
- the data protection officer (where relevant)
- the purposes of the Processing
- a description of the categories of Data Subjects and of the categories of Group Personal Data
- the categories of recipients to whom the Group Personal Data have been or will be disclosed, including recipients in third countries (i.e. outside of the UK or EEA) or international organisations
- where applicable, details of transfers of Group Personal Data to a third country or an international organisation, including the identification of that third country or international organisation and the documentation of suitable safeguards in accordance with Article 49(1)
- where possible, the envisaged time limits for deleting the different categories of Group Personal Data
- where possible, a general description of the technical and organisational security measures in place (as required by Article 32(1)).

All Relevant Parties and Third Parties acting as a Data Processor on our behalf will be required to keep a written record of all categories of Processing activities carried out on our behalf, containing:

- the name and contact details of the Trustee as Data Controller (and each Data Controller) and their name and contact details as Data Processor(s) and, where applicable, of our or their representative, and the data protection officer (if applicable)
- the categories of Processing carried out on our behalf (and each Data Controller generally)
- where applicable, transfers of Group Personal Data to a third country or an international organisation, including the identification of that third country or international organisation and the documentation of suitable safeguards in accordance with Article 49(1)
- where possible, a general description of the technical and organisational security measures referred to in Article 32(1) of the UK GDPR (and Article 32(1) of the EU GDPR if and to the extent applicable).

### 12.2 Privacy by Design and by Default and Impact Assessment

We are required to implement technical and organisational measures to show we have considered and integrated data compliance measures into our Processing activities (known as “data protection by design and by default”).

We commit to this by ensuring that, to the extent possible in respect of Group Personal Data, we and other Relevant Parties and Third Parties:

- identify privacy risks at the outset of any project or before the implementation of a new product, system or service and plan for them accordingly
- in line with the data minimisation principle, pseudonymise, encrypt or anonymise Group Personal Data where possible
- embed privacy into our 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 Group Personal Data.

New products, systems or services developed by Relevant Parties / Third Parties 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 in accordance with the UK GDPR. The Privacy Impact Assessments 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 Group Personal Data and to comply with the UK GDPR (and, if and to the extent applicable, the EU GDPR) generally.

### 13 Personal Data Breach and lost devices

We must report a Personal Data Breach to the Information Commissioner's Office without undue delay (and where feasible within 72 hours), unless the breach is unlikely to result in a risk to the rights and freedoms of the individual and we can demonstrate this. We will also need to inform affected individuals where there is a high risk to their rights and freedoms.

In the event that any Relevant Parties and/or Third Parties become aware of a Personal Data Breach, it has been agreed that:

- they should notify Colin Ross, Group Pensions Manager, within 24 hours and provide as much information as possible (including the nature and the consequences of the Personal Data Breach and any measures taken or proposed to mitigate any adverse effects)
- Colin Ross, Group Pensions Manager will investigate the cause of the Personal Data Breach 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 Personal Data Breach
- where appropriate, the ICO and/or the police must be informed
- the Personal Data Breach must be recorded and, where applicable, the affected individuals informed
- Colin Ross, Group Pensions Manager should also evaluate the effectiveness of the response to the Personal Data Breach and identify any amendments required to this Policy as a result, or to Relevant Parties and Third Parties technical or organisational measures in general.

Should an electronic device or any other storage media containing Group Personal Data be lost or misplaced by the Trustee, please inform Colin Ross, Group Pensions Manager as soon as possible.

## 14 Training and Guidance

All Relevant Parties should implement and ensure that all individuals handling Group Personal Data receive appropriate training on Data Protection Legislation and security requirements, both when initially appointed or engaged and on an ongoing basis.

## 15 Audit

In order to demonstrate compliance with the data protection principles (see section 6) and other applicable requirements under Data Protection Legislation, we will undertake internal audits of our Processing activities from time to time. All Relevant Parties and Third Parties must cooperate with these audits.

## 16 Updates to this Policy

This Policy is the latest version as at June 2026. The information set out in this Policy may change and the Policy may need to be revised. It is also appropriate to review the Policy and the information, processes, decisions and records documented in it from time to time.

This Policy shall be reviewed annually by us, or earlier if required to ensure that it remains up-to-date and fit for purpose.

## 17 Who to contact about this Policy

For questions about this Policy, please contact Colin Ross, Group Pensions Manager, Electricity North West Limited, Borron Street, Stockport, SK1 2JD.