AFFINITY WATER PENSION TRUSTEES LIMITED

Data Protection Principles and Policy

Introduction

Our data protection policy is designed to comply with the **General Data Protection Regulation** ("**GDPR**") and UK **data protection law**, including as applicable to pension schemes, and provides a framework to ensure compliance and best practice. Words highlighted in **bold** are defined in more detail on page 9 of this policy.

By law we must register with the UK Information Commissioner's Office ("**ICO**") as a **controller.** The Plan's **controller** registration number is **Z3603204.** This policy supports our **Privacy Notice**, and both are available at all times to **members** on pensionsWEB.

Affinity Water Pension Trustees Limited ("the Trustee") recognises the importance of respecting the expectations of our **members**, directors, advisors and regulators about how we collect, use, share and dispose of **personal data** (meaning any information (including facts or opinions) that can identify a living person). This policy sets out how we meet these expectations and comply with **GDPR** and UK **data protection law** when handling **personal data**, including **members'** data.

A separate policy and procedure regarding breaches of **GDPR** has been briefed to Trustee directors, officials and advisors and the relevant teams at the Plan's employers. This is contained within the *Administration Procedures Manual*, and is available on the Trustee's document repository and the employers' internal websites for both (Affinity Water Limited ("AWL") and Affinity for Business (Retail) Limited ("**AfB**"). A summary is set out in the Appendix.

Scope: This policy applies to the Affinity Water Pension Plan (the "Plan"), the Trustee, and trustee directors and officials. The Trustee is accountable for implementing the policy and will oversee compliance with the policy. Each trustee director and official is responsible for implementing the policy. AWL's Company Secretary is the Plan and Trustee's **Data Protection Officer** ("**DPO**") and provides advice and guidance to ensure processes, systems and operations are compliant with data protection legislation.

The Trustee will ensure that relevant training and guidance is provided to trustee directors and officials to help them comply with this policy and the law as necessary. Any breach of this policy could result in a breach of **GDPR** and, if misconduct is alleged, be subject to disciplinary action.

GDPR sets out six principles which apply to anyone who obtains, controls, determines or processes **personal data**, whether recorded on paper, computer or electronic device, or recorded calls. These principles, **members'** rights and how the Trustee meets them are set out in this policy.

The Trustee is accountable for ensuring that:

- everyone managing and handling **personal data** is appropriately trained;
- queries regarding **personal data** are dealt with promptly and in accordance with **GDPR** and our **Privacy Notice**;
- methods and procedures for handling **personal data** are regularly assessed and evaluated;
- technical and organisational security measures to safeguard **personal data** are regularly assessed and evaluated to help identify, evaluate and manage risks;
- records are maintained that include clear descriptions of **personal data** types, **data subject** types, **processing** activities, **processing** purposes, third-party recipients of personal data, personal data storage locations, personal data transfers, personal data retention periods, and are kept on a secure data map document; and
- the **DPO** implements and completes **data privacy impact assessments** (when **data processing** presents a high risk to the rights and freedoms of **data subjects**), and ensures the privacy measures implemented are regularly tested (by periodic reviews and audits to assess continuing robust compliance and improvement).

The Trustee reserves the right to change this data protection policy.

Failure to comply with this Policy may mean that **relevant parties** are in breach of their contractual commitments in respect of the Plan.

References to **members** also include beneficiaries and dependants. Reference to "we" may include the Trustee and the Plan administrator (as **Processor**).

Who is a data subject?

Data subjects are defined by **data protection law** as any living individuals whose personal data we process. For us data subjects will include:

- active **members** of the Plan;
- pensioner **members**;
- former **members** of the Plan;
- deferred **members** of the Plan;
- actual and potential beneficiaries (such as spouses, civil partners, children and dependents of **members** of the Plan);
- trustee directors and officials.

Data from third parties

In addition to the information you provide us, we may also receive **personal data** about you from other sources such as:

- your employer;
- solicitors;
- your previous pension scheme/s
- HMRC

See our **Privacy Notice** which explains what personal data we hold, how we use and protect that data, and who we may share the data with.

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 compliance procedures. These are set out in the Appendix (page 6).

How we comply with the data protection principles:

1. PRINCIPLE (a): lawfulness, fairness and transparency

Personal data should be processed lawfully, fairly and in a transparent manner in relation to individuals

1.1 Lawful processing

We will collect, process and share personal data in line with our obligations under applicable data protection law. Our **Privacy Notice** sets out in more detail the lawful basis we rely on to process personal data.

Plan Personal Data

The grounds for **processing personal data** on which we generally rely are:

- Legitimate interests: We have a legitimate interest in **processing personal data t**o ensure the proper administration of the Plan, and to enable the Trustee and relevant third parties (together "**relevant parties**") to calculate and pay benefits. See our **Privacy Notice**
- Compliance with legal obligations: We must meet our trust law duties and responsibilities, and the legal and regulatory requirements affecting pension schemes.

Special Categories of Personal Data

Data protection legislation prohibits the **processing** of **special categories personal data** unless certain conditions are met. The most relevant conditions for us to rely on are:

- Explicit consent: We will always obtain explicit consent when **processing special categories of personal data** from our **members**. Explicit consent requires issuing a **Privacy Notice** to the **data subject** and receiving affirmation from the **member** in writing. We will capture evidence of consent and maintain records of all consents in accordance with **GDPR** and privacy guidelines, in order to safeguard the rights and

freedoms of **members**.

- Information made public: We may **process special categories of personal data** if the **member** has made it manifestly public and if it is necessary for a particular purpose of processing by the relevant parties.

1.2 Fairness and transparency

To satisfy the requirement to be fair and transparent, **relevant parties** will:

- provide members (and any other relevant data subjects) with a fair processing notice, also known as our **Privacy Notice**.
- communicate with **members** (and their dependants and beneficiaries) in a concise and transparent manner using clear and plain language that is easy to understand;
- tell **members** what **personal data** is collected about them, how we intend to use it, who we will share it with, if we intend to transfer it to another country outside the **European Economic Area** ("**EEA**"), as well as letting them know how they can contact the Trustee with questions in order to exercise their rights. We provide our **members** access to this information in our **Privacy Notice**; and
- provide **members** with detailed, specific information, including when data is collected indirectly (for example, from a **third party** or publicly available source), the identity of the **data controller** and **DPO**, and how and why we will use, process, disclose, protect and retain their **personal data** through a **Privacy Notice** (which will be presented when the **member** first provides their personal data).

2. PRINCIPLE (b): 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; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes

2.1 Plan Personal Data

Personal data must only be used for the purposes for which it was collected as set out in Section 1 (also in our **Privacy Notice**).

- **Relevant parties** should only access **personal data** where necessary for the specific purposes set out in the **Privacy Notice**.
- **Relevant parties** should only disclose **personal data** to others within their organisation where the information is needed in order to perform a function within the specified purposes, or as otherwise permitted by the Trustee or required by law.
- **Relevant parties** will not use personal data for new, different or incompatible purposes from that disclosed when it was first obtained without informing **members** of the new purposes, and obtaining their consent where necessary to do so, and updating the **Privacy Notice**.
- In determining whether a new purpose of **processing** is compatible with the original purposes, **relevant parties** will need to consider any link between the purposes, the context in which the **personal data** has been collected, the nature of the **personal data**, the possible consequences of the future **processing** and any proposed safeguards.

3. PRINCIPLE (c): data minimisation

Personal Data should be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed

3.1 Adequate, relevant and limited to what is necessary

Data minimisation means that **relevant parties** must only collect and use the **personal data** needed for the purposes identified in this policy and our Privacy Notice. To do this:

- We will only hold the **personal data** necessary for the Plan's or Trustee's needs or legal requirements;
- We will always ensure that data held is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
- **Relevant parties** will avoid excess copying and/or sharing of **personal data** with other relevant parties where it is not strictly necessary;
- We will ensure that all data is anonymised where practical, and when **personal data** is no longer needed for specified purposes, it will be securely deleted in accordance with our data retention guidance; and
- Any **member** data that trustee directors may hold on **any** approved electronic device will be removed when it is no longer required, and every director will confirm in writing that they have done this, at least annually.

4. PRINCIPLE (d): accuracy

Personal data should be accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay

4.1 Accuracy of data

High quality **personal data** is fundamental to running the Plan.

- **Members** are encouraged to inform the Plan Administrator (or the Plan Company Secretary) of any changes to their **personal data.** See our Privacy Notice for more information. **Relevant parties** will take all reasonable steps to update, rectify or erase records to the extent required without delay. In some cases, it may be necessary to request evidence to support a requested change.

All **relevant parties** will:

- check the accuracy of **personal data** upon collection and at regular intervals;
- ensure the source from which we obtained any personal data is clear and recorded;
- not use **personal data** we suspect might be out of date without confirming its accuracy;
- take reasonable steps to ensure that inaccurate **personal data** is corrected or securely deleted without delay; and
- provide the Trustee with reports on the accuracy of **personal data** and how it is being monitored.

5. PRINCIPLE (e): storage limitation

Personal data should be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals

To meet the requirements of UK tax and pensions law, we must keep certain **personal data** for many years. We will review **personal data** on a regular basis.

5.1 Storage

- Given the long-term nature of pension schemes, we consider that it is necessary to keep **personal data** for at least the **member's** life time plus 20 years - **data subjects** are informed of this in our Privacy Notice;

- This period reflects the potential for queries and complaints in relation to the Plan many years after an individual has ceased to be a **member**;
- **Personal** d**ata** will be securely archived and only accessible by a restricted group of authorised persons;
- If the Trustee concludes that certain **personal data** is no longer needed, that data will be destroyed in accordance with our data retention guidance; and
- We will regularly review and maintain data retention guidance to ensure **personal data** is deleted in line with legal requirements as required for a pension scheme.

5.2 Relevant parties

The Trustee will ensure that:

- **Relevant parties** regularly review **personal data** held on its behalf and take appropriate steps to delete, destroy or prevent access to **personal data** that is no longer required; all such actions will be undertaken securely and permanently.
- Where **personal data** is used by **relevant parties** for the purposes of communicating with members, it may be retained by the **relevant parties** for a maximum period of six months (in order, for example, to respond accurately and promptly to queries) after which it must be deleted.

6. PRINCIPLE (f): security, 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

We will maintain data security by protecting the confidentiality, integrity and availability of all **personal data**:

- Confidentiality**:** only people who have a need to know and are authorised to use the personal data can access it;
- Integrity: ensure access is limited and data is protected from loss or corruption;
- Availability: authorised users can access the personal data when they need it for authorised purpose;
- We will ensure, that administrative, physical and technical safeguards are implemented and maintained in accordance with **GDPR** and relevant standards to protect **personal data.**

All **relevant parties** must observe the following requirements to keep **personal data** confidential and secure:

6.1 Security

Personal data will be kept, processed and shared securely by the Trustee and **related parties** from when it is first collected until its eventual destruction.

- The Trustee and all **relevant parties** will ensure that appropriate technical and organisational measures are in place to protect **personal data** against unauthorised or unlawful **processing**, and against any loss, destruction or damage, including appropriate physical and technical security and robust policies and procedures;
- **Personal data** will only be transferred to **relevant parties** who have confirmed that they have appropriate measures in place or who agree to put them in place;
- **The Trustee** will ensure a robust compliance monitoring framework is in place to audit **relevant parties,** in order to independently demonstrate compliance with **DP legislation**;
- Clear security measures are in place for the transfer of any personal and sensitive data onto electronic devices (or by post).
- The requirement to keep **personal data** confidential and safe applies regardless of how the information is held e.g. laptops, other portable devices, desktops, disks, USBs, as part of a database, in paper form or otherwise.

6.2 Access

- Access to **personal data** must only be given to those who have a genuine need to access such **data** to carry out their duties; and
- Appropriate audit trails will be put in place to monitor access and amendments to records to ensure accountability**.**

6.3 Physical security and storage of documents

- All information used will be stored safely and securely by using secure filing cabinets, access controls, passwords, etc; and
- Paper documents should be disposed of as confidential waste or shredded.

6.4 Storage of electronic personal data

All electronic **personal data** will be stored on a secure network or on a computer with the appropriate security software installed, which should be regularly updated, with access controls (eg user ID and passwords) in place. This includes off-site working and use of own devices.

6.5 Sharing data with relevant parties

Personal data will only be shared with other **relevant parties** if certain safeguards and contractual arrangements have been put in place:

- we have a lawful basis for sharing the **personal data**;
- they have a need to know the information for the purposes of providing contractual services;
- sharing the personal data complies with the **Privacy Notice** provided to the **data subject**
- they have agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
- the transfer complies with any applicable cross border transfer restrictions; and
- a fully-executed written contract that contains clauses that comply with applicable data protection laws has been obtained.

6.6 Sharing data with third parties

We will only share **personal data** with other **third parties** if certain safeguards and contractual arrangements have been put in place:

- they have a need to know the information for the purposes of providing contractual or other legal services to members;
- sharing the personal data complies with the **Privacy Notice** provided to the **data subject** and, if required, the **data subject**'s consent has been obtained; and
- they have agreed to comply with DP legislation

- This policy was approved by the Affinity Water Pension Trustees Limited Board on 27 March 2019

Signed

Chair of the Trustee

APPENDIX

1. Personal data breach and lost devices

This is a summary of the Trustee's Breaches Policy and Procedure, which is available on request from the Company Secretary:

We must report a **personal data breach** to the **ICO** without undue delay and within 72 hours unless the breach is unlikely to result in a risk to the rights and freedoms of the individual/s, and we are able to demonstrate this.

If anyone knows or suspects that a **personal data breach** has occurred, they must immediately notify the Trustee DPO and the Trustee Company Secretary at pensiontrustee@affinitywater.co.uk and ensure they preserve all evidence relating to the potential breach.

If any **relevant parties** become aware of a **personal data breach**:

- Notify the Trustee Company Secretary within 24 hours and provide as much information as possible, including the nature and the consequence of the **breach** and any measures taken or proposed to mitigate any adverse effects;
- The Company Secretary and Trustee **DPO** will investigate the cause of the **breach** and assess the risk to members, then recommend to the Trustee what action needs to be taken to recover any losses and to limit the damage caused by the **breach**;
- Where appropriate, the **ICO** and/or the Police must be informed – the Trustee will decide whether or not to inform the ICO and/or Police;
- The **breach** must be recorded in the Trustee's breaches log;
- We will inform affected individuals where there is a high risk to their rights and freedoms; and
- The Trustee Company Secretary will prepare a report that enables the Trustee to evaluate the effectiveness of the response to the **breach** and identify any amendments required to this policy or to the controls operated by the Trustee or **relevant parties**.

Should an electronic device or any other storage media containing **personal data** be lost or misplaced by any relevant party, the Company Secretary to the Trustee should be notified as soon as possible.

2. Transfer limitation

GDPR restricts data transfers to countries outside the **EEA** to ensure that the level of data protection afforded to individuals by **GDPR** is not undermined. We will only transfer **personal data** outside the **EEA** to countries having an adequate level of protection for the rights and freedoms of **data subjects** in relation to the **processing** of **personal data** by ensuring that at least one of the following conditions applies:

- the European Commission ("EC") has issued a decision confirming that the country has an adequate level of protection for **members'** rights and freedoms;
- appropriate safeguards must exist such as binding corporate rules or standard contractual clauses approved by the EC;
- the **member** must provide explicit consent to the proposed transfer after being informed of any potential risks; and
- the transfer must be necessary for one of the reasons set out in **GDPR** including the performance of a contract between the Trustee and the data subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the data subject where the data subject is physically or legally incapable of giving consent and, in some limited cases, for the Trustees' legitimate interest.

3. Data subjects' rights and requests

Members can exercise certain rights about their **personal data.** The Trustee will always protect individual's rights under **DP legislation** (to the extent applicable).

3.1 Members' rights: As set out in our **Privacy Notice**, we will:

- not disclose **members' personal data** to **third parties** without proper authorisation;
- verify the identity of any individual requesting data;
- forward any **data subject** request received to the Company Secretary

in the first instance, who will comply with the Trustee **data subject** response process;
- respond to **member** requests to see what information is held about them in a timely manner;
- adhere to **GDPR** requirements when considering **members'** request to stop or prevent **processing**;
- adhere to **GDPR** requirements when considering any claim for compensation relating to damage or distress caused by a breach of **personal data**; and
- consider any requests from **members** to receive their **personal data** or, in limited circumstances, to transfer data to a third party, and supply data in a commonly used and machine-readable format.

3.2 Members' Requests: Regarding how we handle their **personal data** as set out in our **Privacy Notice**, **members** have rights to:
- withdraw consent to **processing** at any time;
- request access to their **personal data** the Trustee holds;
- prevent our use of their **personal data** for direct marketing purposes;
- ask the Trustee to erase **personal data** if it is no longer necessary for the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data;
- challenge **processing** which has been justified on the basis of our legitimate interests or in the public interest;
- request a copy of an agreement under which **personal data** is transferred outside of the **EEA**;
- object to decisions based solely on **automated processing**;
- prevent **processing** that is likely to cause damage or distress to the data subject or anyone else; and
- be notified of a **personal data** breach which is likely to result in high risk to their rights and freedoms.

4. Training and guidance

Relevant parties should ensure that all individuals handling **personal data** receive appropriate training on **DP legislation** and security requirements, both when initially appointed or engaged and on an ongoing basis.

5. Audit

To demonstrate compliance with the Data Protection principles and all other applicable requirements under **DP legislation**, the Trustee will undertake internal audits of our **processing** activities from time to time. All **relevant parties** must cooperate with these audits.

6. Updates to this policy

The latest version of this policy is available on pensionsWEB. The information set out in this policy may change and the policy may need to be revised. The Trustee will review the policy and the information, processes, decisions and records documented at appropriate intervals to ensure that it remains up-to-date and fit for purpose.

7. Record-keeping

Full and accurate records will be kept of all **processing** including: records of **data subject** consents: the name and contact details of the **Data Controller** and **DPO**; and clear descriptions of the **personal data** types, **processing** activities, **processing** purposes, third-party recipients of **personal data**, **personal data** storage locations, **personal data** transfers, **personal data** retention periods, and security measures in place.

8. Who to contact about this policy

For questions regarding this policy, please contact the Trustee Company Secretary at pensiontrustee@affinitywater.co.uk

DEFINITIONS

Automated decision-making ("ADM")	When a decision is made which is based solely on automated **processing** (including profiling) which produces legal effects or significantly affects an individual. The **GDPR** prohibits ASM (unless certain conditions are met) but not automated **processing**.
Automated processing	Any form of automated **processing** of **personal data** consisting of the use of **personal data** to evaluate certain personal aspects relating to an individual, to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
Company	Affinity Water Pension Trustees Limited
Consent	Agreement which must be freely given, specific, informed and be an unambiguous indication of the data subjects' wishes by which they, by a statement or by a clear positive action, signifies agreement to the **processing** of **personal data** relating to them.
Criminal convictions date	Means **personal data** that relates to criminal convictions and offences
Data subject	A living, identifiable individual about whom the Trustee holds **personal data**. Data subjects may be nationals or residents of any country and may have legal right regarding their **personal data**.
Data privacy impact assessment ("DPIA")	Tools and assessments used to identify and reduce risks of a data **processing** activity. DPIA can be carried out as part of privacy by design and should be conducted for all major system or business change programmes involving the **processing** of **personal data**.
Data controller	The person/s or organisation that determines when, why and how to process **personal data**. Responsible for establishing practices and policies in line with **GDPR**. The Trustee and its administrator are data controllers of **personal data relating to the Plan and Trustee**.
Data processor	Means any legal or natural person that processes **personal data** on behalf of the **data controller**, for example, the Plan administrators
Data protection ("DP") legislation/law	Means, as applicable, the EU Data Protection Directive (95/46/EU) and any legislation and/or regulation implementing or made pursuant to it (including the Data Protection Act 1998), the **GDPR** and any legislation and/or regulation implementing or made pursuant to it, together with any law or regulation which amends, replaces, supplements or consolidates any of the foregoing from time to time.
Data Protection Officer ("DPO")	The person required to be appointed in specific circumstances under **GDPR**.
EEA	Countries in the European Union, Iceland, Lichtenstein and Norway.
Explicit consent	Consent which requires a very clear and specific statement (ie not just action).
General Data Protection Regulation ("GDPR")	The General Data Protection Regulation (EU) 2016/679. **Personal data** is subject to the legal safeguards specified in **GDPR**.
ICO	Means the **Information Commissioner's Office**, the UK regulatory body charged with ensuring compliance with data protection legislation.
Member/s	Includes current Plan **members**, current and potential beneficiaries, deferred **members**, pension **members** and former **members**.
Personal data	Any information identifying a **data subject** or information relating to a data subject that we can identify (directly or indirectly) from that data alone, or in combination with other identifiers the Trustee possess or can reasonably access. **Personal data** includes **special categories of personal data** and pseudonymised **personal data** but excludes anonymous data or data that has the identity of an individual permanently removed. **Personal data** can be factual (eg a name, email address, location or date of birth), or an opinion about that person's actions or behaviour.
Personal data breach	Any act or omission that compromises the security, confidentiality, integrity or availability of **personal data** or the physical, technical, administrative or organisational safeguards that we or our service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of **personal data** is a **personal data breach**.
Privacy by design	Implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the **GDPR**.
Privacy Notice	Separate notices setting out information that may be provided to data subjects when the Company collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (eg

	employee privacy notices or the website privacy policy) or they may be stand-alone, one-time privacy statements covering **processing** related to a specific purpose.
Processing or process	Any activity that involves the use of **personal data**. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. **Processing** also includes transmitting or transferring **personal data** to **third parties**.
Pseudonymisation	Replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the **member** to whom the data relates cannot be identified without the use of additional information which is kept separately and secure.
Related policies	The Trustee's policies, operating procedures or processes related to this policy and designed to protect **personal data**.
Relevant parties	A collective term that applies to the Trustee, trustee directors and officials; Employers and their employees; and advisors and their employees who provide support to the Plan or who have access to **personal data** relating to the Plan or Trustee and may, from time to time, require **personal data** from the Plan in accordance with **DP legislation**, this policy and related policies.
Sensitive personal data	Information about a person's personal, family or professional life, including medical data and criminal convictions data.
Special categories of personal data	Information revealing racial or ethnic origin, political opinions, sexual life, sexual orientation, biometric or genetic data.
Third parties	Any third party that may, from time to time, require **personal data** from the Plan in accordance with **DP legislation**, this policy and related policies (eg HMRC, members' appointed IFAs).