

Affinity Water Pension Trustees Limited on behalf of the Affinity Water Pension Plan Data Protection Policy

Introduction

Affinity Water Pension Trustees Limited ("the Trustee") is responsible for the administration of the Affinity Water Pension Plan ("the Plan").

We have adopted the Data Protection Policy of the Plan's principal employer, Affinity Water Limited, as our documents and records are held on that company's premises and systems.

The current policy is set out overleaf.

GDPR

We are in the process of revising our Data Protection Policy to reflect the requirements of the General Data Protection Regulations, which come into force on 25 May 2018.

It is planned that the revised policy will be approved by the Trustee Board at its next meeting on 6 June 2018.

We will replace this current policy with the revised policy at that time.

Contact

If you have any questions about the policy, please contact us at pensiontrustee@affinitywater.co.uk

1. At Affinity Water, we recognise the importance of respecting the expectations of our customers, employees and others about how we collect, use, share and dispose of their personal data (meaning any fact or opinion about a living person). This policy sets out how we meet their expectations and comply with the Data Protection Act 1998.
2. This policy applies to all employees (including contract staff) of Affinity Water Limited. The Information Security Board, supported by the Information Security Forum, will oversee compliance with this policy. Each director is accountable to the Information Security Board for implementing this policy in their business area. The Company Secretary is our Data Protection Officer and provides advice and guidance to ensure processes, systems and operations are compliant with data protection legislation.
3. We provide training and issue guidance to help you comply with this policy and the law. Any breach of this policy or guidance could amount to misconduct, and therefore be subject to Affinity Water's disciplinary policy.
4. The Data Protection Act 1998 sets out eight principles which apply to anyone who obtains and controls personal data, whether recorded on paper, on computer, or recorded calls. It also provides individuals a number of rights in respect of their personal data. These principles and rights (and how Affinity Water meets them) are set out below.

Principle 1 – Fairly and lawfully processed

- We collect and use personal data fairly and lawfully
- We are transparent about how we use personal data
- We handle people's personal data only in ways they would reasonably expect
- we only use customers' personal data to market non-water related services and products, if they have opted in and agreed to how we will market these products and services to them
- We obtain consent to collect and use sensitive personal data (meaning information about a person's personal, family or professional life).

Principle 2 - Processing only for a specific purpose

- We specify the purpose(s) of collecting and using personal data:
 - We give privacy notices when we collect personal data and register the purposes for which we use personal data with the Information Commissioner
 - We publish guidance for our customers on how we use and protect their personal data. We explain that we might share their personal data with their wastewater company, our regulators, government agencies and credit reference agencies

Principle 3 - Adequate, relevant and not excessive

- We hold sufficient (but not excessive) personal data for our business needs
- We hold personal data that is sufficient for the purpose we are holding it for and will not hold more information than we need for that purpose

Principle 4 - Accurate

- We take reasonable steps to ensure the accuracy of personal data we hold
- We ensure the source from which we obtained any personal data is clear and recorded
- We consider any challenges to the accuracy of information and whether it is necessary to update it

Principle 5 - Kept no longer than necessary

- We retain personal data no longer than we need
- We determine for each purpose we hold personal data how long we need to retain it
- We securely delete or destroy personal data that is no longer needed
- We update personal data if it goes out of date

Principle 6 - Processed in accordance with individuals' rights

- We respect the rights of individuals under the Data Protection Act 1998 to:
 - have a copy of the personal data we hold about them (for example information we have recorded about customers on their account), by requesting this in writing and paying a fee of £10
 - object to processing that is causing (or is likely to cause) them damage or distress
 - prevent processing for direct marketing
 - object to decisions being taken by automated means
 - have inaccurate personal data rectified, blocked, erased or destroyed

Principle 7 – Kept secure

- We keep personal data secure through technical and organisational controls
- We design and organise our security procedures to fit the nature of the personal data we hold and the harm that may result from a security breach
- We are clear who is responsible for ensuring personal data is kept secure
- We make sure we have the right physical and technical security, backed up by robust policies and procedures and well-trained employees
- We are ready to respond to any breach of security swiftly and effectively

Principle 8 - kept protected if it's sent to another country

- We only transfer personal data outside the European Economic Area to countries having an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data