

THE ARBOLEAS HOME WATCH (AHW) - DATA PROTECTION POLICY updated 08/05/2018

The Data Protection Principles - Personal Data

Cover any data which can be used to identify a living person. This includes names, dates of birth, references (NIE, Residency, Passport, NINo), addresses, telephone numbers and email addresses. It only applies to that data which is held or intended to be held on computers or in a relevant filing system.

The Act and Regulations have been updated and superceded by General Data Protection Regulation (GDPR) in the European Union which comes into effect on 25th May 2018.

A Statement to Members of AHW

The new GDPR regulations provide the legal framework that defines how personal information can be used. The Act is based on eight principles. The AHW Policy for Data Protection is set out in the following statement. The AHW is fully committed to compliance with the regulations. The following principles will be applied when we handle your personal information:

- Your personal information is only used with your knowledge;
- Only information that we actually need is collected;
- Your personal information is only seen by those who need it to do their roles;
- We will not pass your personal information on to any other organisation without your agreement, unless required to do so by the law;
- Personal information is retained only for as long as it is required;
- We will, where necessary, keep your information up-to-date;
- Your information will be protected from unauthorised or accidental disclosure;
- We will provide you with a copy of your personal information on request when we hold it;
- Inaccurate or misleading data will be corrected as soon as possible;
- A "right to be forgotten": When an individual no longer wants her/his data to be processed, and provided that there are no legitimate grounds for retaining it, the data will be deleted.
- The use of the BCC facility in emails will be used to help protect private computer systems.

These principles apply whether we hold your information on paper or in electronic form.

Our Obligations

- To collect, use, store and dispose of personal information in accordance with the principles set out.
- To respect and grant the rights of individuals set out.
- To ensure all who are contracted to process our data comply.
- To provide scheme membership awareness of data protection.

Individuals' Rights: Individuals (known as Data Subjects) have four main rights:

1. A right to see what data is held about them.
2. A right, at any time, to prevent use of their data for direct marketing purposes.
3. A right to prevent processing of their data which is likely to cause damage or distress.
4. A right to have inaccurate data corrected and the right to be forgotten.

The Data Protection Principles

The eight Data Protection Principles are the heart of the European Data Protection Directive. They set out a basic code which should be followed by anybody handling personal information.

Personal information includes computerised, audio and video records, as well as structured manual records from which living individuals may be identified. Further specific requirements, rights for individuals and penalties for non-compliance are set out in the Directive.

The First Principle

Personal information shall be processed fairly and lawfully.

The Second Principle

Personal information shall only be obtained for one or more specified and lawful purposes, and must not be used in any manner that would be inconsistent with these purposes.

The Third Principle

Personal information shall be adequate, relevant and not excessive in relation to the purpose(s) for which it is processed

The Fourth Principle

Personal information must be accurate and, where necessary, kept up to date

The Fifth Principle

Personal information processed for any purpose(s) must not be kept for longer than is necessary for that purpose or purposes.

The Sixth Principle

Personal information must be processed in accordance with the rights of the data subjects as defined in the Act (see box for individuals' rights)

The Seventh Principle

Appropriate technical, procedural and organisational measures shall be taken against unauthorised or unlawful processing and against accidental loss, destruction or damage of personal information.

The Eighth Principle

Personal information shall not be transferred to a country outside the EEA (EEC plus Norway, Iceland and Liechtenstein) unless that country or territory provides an equivalent level of protection or the data subject gives explicit consent to the transfer.

Complying with the Act

The Act imposes obligations on us to those whose information we hold. It applies to both paper and electronic records. For anyone who handles personal information the key points to remember are:

- Identify all of your holdings of personal data and what use is made of them; if you hold data you no longer use, erase it.
- Ensure that everyone you hold data about:
 - Knows what you are holding;
 - Why you are holding it;
 - How you are holding it;
 - How you might use it; And to whom it might be passed;
- Keep data securely;
- Remember that the people you hold data on have a right to see it;
- If in doubt ask for advice.
- Don't introduce any new system for processing of personal data without due regard for data protection requirements.