

# OUTWEST

## Data Management Policy

Effective from 1st February 2010

*Amended 30<sup>th</sup> January 2010, Eastbourne*

*All amendments have been italicized*

### Handling Membership Data

#### 1. Introduction

The intention of this policy is to make all members aware of the principles that govern the obtaining, use, storage and destruction of member's personal data. This policy will explain member rights and responsibilities under the Data Protection Act 1998 (DPA), including the criminal offences established by the DPA.

#### 2. Policy Statement

As part of its *voluntary* compliance with the DPA, this policy sets out the requirements to ensure that all members are aware of their legal rights and responsibilities under the DPA with regard to members' personal data. It is the policy of OutWest to define these rights and responsibilities in respect of collecting, storing, organizing, retrieving, altering, disclosing and destroying the personal data of its membership.

Failure to comply with this policy could lead to action being taken under *OutWest's Grievance Procedure* which may result in the removal of a Trustee or member. In some cases, criminal *or civil* prosecution *could* also be a possibility.

#### 3. Requirements

As an organisation OutWest needs to collect information about members in order to manage and conduct its business. The DPA governs how this happens and provides rules for the use of that information. This section explains what is covered by the term personal data and outlines the rights of members, the responsibilities of the organisation, all members and trustees, and the criminal offences established by the DPA. It will also explain the interface between the Freedom of Information Act and the Data Protection Act.

#### Personal Data

The DPA defines 'personal data' as data relating to a living individual who can be identified:

- from that data; or
- from that data and other information which is in the possession of, or is likely to come into the possession of the trustees or organisation.

In addition:

- the individual must be the focus of the information concerned; and
- the information has to tell you something of significance about that individual.

This definition includes any expression of opinion about the individual and any indication of the intentions of the organization or any other person in respect of the individual.

### **Sensitive Personal Data**

The DPA identifies a set of personal information which is particularly sensitive and can only be processed in certain limited circumstances (for example, with the explicit consent of the individual concerned, or if employment law imposes a specific obligation to carry out the processing). This sensitive personal data is defined as information concerning:

- their racial or ethnic origin
- their political opinions
- their religious beliefs or other beliefs of a similar nature
- their physical or mental health or condition
- their sexual *orientation*
- *their age*
- the commission or alleged commission of any offence,
- proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings

### **Rights**

Any living person whose personal data is being held by an organization has the following rights under the DPA:

- to know whether their data is being processed
- to make a subject access request in writing to see any of their data held by that organisation, including the purposes for which it is held, the source of the information and the types of organization to which it may be disclosed
- to have the data supplied to them in an intelligible form
- to have any inaccuracies corrected or destroyed
- to have their data held securely and not disclosed unlawfully
- to prevent the processing of their data if that processing is likely to cause substantial and unwarranted damage or distress
- to claim compensation for loss and damage if their data is misused or wrongly disclosed

OutWest will not normally request payment for a subject access request that is made by a current member of OutWest.

**Responsibilities:**

OutWest will collect, use, store, organise, retrieve, alter or destroy member personal data in compliance with the DPA by:

- obtaining personal data (including sensitive personal data) only for specified and lawful purposes and not processing data in a way that is incompatible with those purposes
- informing members of the purpose for which their data will be used
- processing personal data for limited purposes, as published on the Information Commissioner's Public Register of Data controllers ([www.ico.gov.uk](http://www.ico.gov.uk))
- obtaining only data relevant to a specific and stated purpose
- keeping any collected personal data up to date, where it is necessary to do so
- destroying personal data when it is no longer necessary for the purpose for which it was collected.
- applying the rights of members under the DPA, as explained under the 'Rights' section of this policy
- taking all reasonably practical measures to ensure the physical, technical and organisational security of the personal data, including appropriate contractual safeguards when outsourcing
- transferring personal data abroad only if satisfied that it will be protected to UK standards
- take steps to comply with the requirements outlined in this policy in respect of their areas of responsibility, in accordance with the supporting guidelines
- ensure that all trustees working in their areas of responsibility are aware of their rights and responsibilities under this policy and the DPA

*The Co-chair (Events and Administration) is responsible for ensuring that OutWest has the necessary framework in place to achieve compliance with the DPA.*

*OutWest have voluntarily registered the Co-Chair (Events and Administration) with the Information Commissioners Office (ICO) as OutWest's designated Data Controller, and will update the ICO if there is a change in Co-Chair (Events and Administration).*

**Criminal Offences**

The DPA establishes criminal offences for individual and deliberate misuse of personal data. It is an offence for any member of OutWest to unofficially:

- obtain or disclose another person's personal data, or
- procure the disclosure of another person's personal data to a third party
- sell another person's personal data

It is not a criminal offence to disclose personal data if the disclosure: is in response to a court order, is expressly required by a piece of legislation, is carried out with the consent of the individual concerned, or is carried out in connection with the prevention or detection of a crime.

It is a criminal offence to destroy or conceal personal data whose disclosure has been requested through a subject access request, if this is done with the intention of preventing its disclosure to the individual concerned.

In all cases members should contact the Secretary or the Co-chair (Events and Administration) before undertaking any of these activities.

### **Freedom of Information**

The Freedom of Information Act 2000 (Fol) allows individuals to request access to certain types of information held by public organizations like OutWest. The vast majority of personal data is exempt from disclosure in response to such requests. However, some personal data will be considered for disclosure in accordance with the following principles:

- if information relates to the professional aspects of an member's role within OutWest (eg a decision they have *individually or been part of a collective* made, or a report they have written) then the information is likely to be disclosed
- the more senior an member, the more likely it if that information about them and the performance of their role at OutWest will be disclosed.

Sensitive information or information that could cause damage or distress if released (eg a member's health record or home address) will not be disclosed under Freedom of Information.

### **Breaches of this Policy**

Any failure to comply with this policy may lead to action being taken under OutWest's Grievance Policy and Procedure which may result in membership being revoked without notice.

Members should also be aware that they could be committing a criminal offence or causing OutWest to commit a criminal *or civil* offence by not complying with this policy.

### **4. Support and advice**

Support and advice can be obtained through speaking to the Co-chair (Events and Administration).

Additional guidance for trustees on the specific area of member subject access (the right of members to request access to information about themselves held by OutWest) is available upon request.

Any complaints about the way in which OutWest processes personal information (or its failure to comply with the provisions of the DPA) should be passed to the Co-chair (Events and Administration), who will ensure that such complaints are fully investigated.

The Information Commissioner's Office is an external regulator who monitors compliance with the Data Protection and Freedom of Information Acts and investigates alleged breaches of these two pieces of legislation. They can be contacted via a telephone help line: 01625 545745, or at the following address: Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 SAF. Their website address is: [www.ico.gov.uk](http://www.ico.gov.uk)