



Data Protection Policy

for

The Astor Bannerman Group of Companies

Issue Date: 3rd January 2014
Version: 01

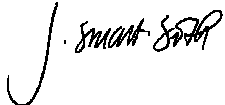

Approval History				
Name	Department	Role/Position	Date approved	Signature
James Stuart-Smith	Director	Managing Director	3 rd January 2014	
Peter Deverson	Director	Technical Director	3 rd January 2014	

Table of Contents:

Paragraph	Subject
1	Aims of this Policy
2	Definitions
3	Type of Information Processed
4	Notification
5	Responsibilities
6	Policy Implementation
7	Training
8	Gathering and Checking Information
9	Data Security
10	Subject Access Requests
11	Review

1 Aims of this Policy

The Astor Bannerman Group of Companies needs to keep certain information on its Employees and Business Partners including Leads, Customers, Clients and Suppliers to carry out its day to day operations, to meet its objectives and to comply with legal obligations.

The organisation is committed to ensuring any personal data will be dealt with in line with the Data Protection Act 1998 (DPA). To comply with the law, personal information will be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

The aim of this policy is to ensure that everyone handling personal data is fully aware of the requirements and acts in accordance with data protection procedures. This document also highlights key data protection procedures within the organisation.

This policy covers all employed staff including temporary staff and consultants.

[Back to Table of Contents](#)

2 Definitions

In line with the Data Protection Act 1998 principles, The Astor Bannerman Group of Companies will ensure that personal data will:

- 1 Be obtained fairly and lawfully and shall not be processed unless certain conditions are met
- 2 Be obtained for a specific and lawful purpose
- 3 Be adequate, relevant but not excessive
- 4 Be accurate and kept up to date
- 5 Not be held longer than necessary
- 6 Be processed in accordance with the rights of data subjects
- 7 Be subject to appropriate security measures
- 8 Not to be transferred outside the European Economic Area (EEA)

The definition of 'Processing' is obtaining, using, holding, amending, disclosing, destroying and deleting personal data. This includes some paper based personal data as well as that kept on computer.

The Personal Data Guardianship Code suggests five key principles of good data governance on which best practice is based. The organisation will seek to abide by this code in relation to all the personal data it processes, i.e.

- **Accountability:** those handling personal data follow publicised data principles to help gain public trust and safeguard personal data.
- **Visibility:** Data subjects should have access to the information about themselves that an organisation holds. This includes the right to have incorrect personal data corrected and to know who has had access to this data.
- **Consent:** The collection and use of personal data must be fair and lawful and in accordance with the DPA's eight data protection principles as identified above. Personal data should only be used for the purposes agreed by the data subject. If personal data is to be shared with a third party or used for another purpose, the data subject's consent should be explicitly obtained.
- **Access:** Everyone should have the right to know the roles and groups of people within an organisation who have access to their personal data and who has used this data.
- **Stewardship:** Those collecting personal data have a duty of care to protect this data throughout the data life span.

[Back to Table of Contents](#)

3 Type of Information Processed

The Astor Bannerman Group of Companies processes the following personal information:

- Information on applicants for employment positions, including references.
- Employee information – contact details, bank account number, payroll information, supervision and appraisal notes.
- Business Partner information – contact details, banking details, addresses.
- Client Information – contact details, details of equipment installed, addresses.

All Personal information is kept either electronically within the organisations database or within the paper based filing system.

Personal Information held within the organisation is accessed only by designated employees. Sensitive Personal Information such as ethnic origin, political opinions, religious beliefs, membership of a trade union, physical or mental health, criminal convictions is held within the Accounts/Personnel Department and is secured either by electronic permissions or secure filing cabinets.

[Back to Table of Contents](#)

4 Notification

The requirements we have for processing personal data are recorded on the public register maintained by the Information Commissioner. We notify and renew our notification as the law requires.

If there are any interim changes, these will be notified to the Information Commissioner within 28 days.

The name of the Data Controller within our organisation as specified in our notification to the Information Commissioner is Tony Taylor.

[Back to Table of Contents](#)

5 Responsibilities

Under the Data Protection Guardianship Code, overall responsibility for personal data rests with the Managing Director. In the case of The Astor Bannerman Group of Companies, this is James Stuart-Smith.

The Managing Director delegates tasks to the Data Controller. The Data Controller is responsible for:

- understanding and communicating obligations under the Act
- identifying potential problem areas or risks
- producing clear and effective procedures
- notifying and annually renewing notification to the Information Commissioner, plus notifying of any relevant interim changes

All employees who process personal information must ensure they not only understand but also act in line with this policy and the data protection principles.

Breach of this policy may result in disciplinary proceeding.

[Back to Table of Contents](#)

6 Policy Implementation

To meet our responsibilities, employees will:

- Ensure any personal data is collected in a fair and lawful way;
- Explain why it is needed at the start;
- Ensure that only the minimum amount of information needed is collected and used;
- Ensure the information used is up to date and accurate;
- Review the length of time information is held;
- Ensure it is kept safely;
- Ensure the rights people have in relation to their personal data can be exercised

We will ensure that:

- Everyone managing and handling personal information is trained to do so.
- Anyone wanting to make enquiries about handling personal information, whether a member of staff, volunteer or service user, knows what to do;
- Any disclosure of personal data will be in line with our procedures.
- Queries about handling personal information will be dealt with within the 40 days required by the DPA from receiving the written request (and relevant fee).

[Back to Table of Contents](#)

7 Training

Training and awareness raising about the Data Protection Act and how it is followed in this organisation will take the following forms:

On induction: A copy of this policy is provided and the employee signs an induction form to confirm that they have received and understood the policy.

Also on induction, staff are provided with relevant training relating to any paper based filing systems that they are authorised to access.

Staff are also provided with a copy of The Astor Bannerman Group of Companies I.T Acceptable Use Policy for which they sign the Induction form to confirm that they have read and understood it. The IT Acceptable Use Policy details requirements for ensuring that all information held within the organisations IT System is secure at all time.

General training/ awareness raising: Further awareness training is carried out during regular departmental meetings.

[Back to Table of Contents](#)

8 Gathering and Checking Information

Before personal information is collected, we will consider:

- What details are necessary for your purposes?
- How long you are likely to need this information?

We will inform people whose information is gathered about the following:

- Why the information is being gathered?
- What the information will be used for?
- Who will have access to their information (including third parties)?

We will take the following measures to ensure that personal information kept is accurate:

- Periodic reviews of our Business Partner database will be carried out to identify obsolete records. Obsolete records will be deleted in accordance with the organisations Document Control Procedure contained within the Quality Manual.
- Client's details will be kept up to date by means of regular letters being sent out requesting them to update their information.
- On completion of providing a service to clients, they will be contacted to offer a further period of service or given the option to request that their details be removed from the organisations database.

Personal sensitive information will not be used apart from the exact purpose for which permission was given.

[Back to Table of Contents](#)

9 Data Security

The organisation will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure. The following measures will be taken.

- Using lockable cupboards (restricted access to keys)
- Password permissions protection on personal information files
- Setting up computer systems to allow restricted access to certain areas
- Not allowing personal data to be taken off site.
- Back up of data on computers (onto a separate hard drive / onto tapes kept off site)
- Compliance with the organisations IT Acceptable Use Policy.

Any unauthorised disclosure of personal data to a third party by an employee may result in disciplinary proceedings.

Any unauthorised disclosure of personal data to a third party by a volunteer or trustee may result in disciplinary proceedings.

[Back to Table of Contents](#)

10 Subject Access Requests

Anyone whose personal information we process has the right to know:

- What information we hold and process on them
- How to gain access to this information
- How to keep it up to date
- What we are doing to comply with the Act.

They also have the right to prevent processing of their personal data in some circumstances and the right to correct, rectify, block or erase information regarded as wrong.

Individuals have a right under the Act to access certain personal data being kept about them on computer and certain files. Any person wishing to exercise this right should apply in writing to:

Tony Taylor
The Data Controller
The Astor Bannerman Group of Companies
Unit 11f Coln Park
Andoversford
Cheltenham
Gloucestershire
GL54 4HJ

We may make a charge of £10 on each occasion access is requested.

The following information will be required before access is granted:

- Full name and contact details of the person making the request
- Their relationship with the organisation (former/ current member of staff, Business Partner, Service User, etc.
- Address of where we supplied equipment to or provided any service at.

We will also require proof of identity before access is granted. The following forms of ID will be required:

- Passport, Driving License, or Birth Certificate

Queries about handling personal information will be dealt with swiftly and politely. We will aim to comply with requests for access to personal information as soon as possible, but will ensure it is provided within the 40 days required by the Act from receiving the written request (and relevant fee).

[Back to Table of Contents](#)

11 Review

This policy remains under constant review and is discussed at each senior management meeting to ensure it remains up to date and compliant with the law.

[Back to Table of Contents](#)