



The
British
Psychological
Society

Data Protection Policy

For use in:	All Society functions
For use by:	All staff
Owner:	Corporate Services
To be used in conjunction with:	Various working practises
Date of Approval:	31 August 2012
Approved by:	SMT
Launch Date:	3 September 2012
Review Date:	August 2013

Introduction

The Data Protection Act 1988 places a number of responsibilities upon people and organisations who use personal information, and gives rights to individuals to control the use of their personal data and to obtain a copy of it. In particular the Act sets out eight principles that govern how information is obtained, stored, and disclosed:

1. fairly and lawfully processed;
2. only obtained for one or more specified lawful purposes, and processed only for those purposes;
3. only held if it is relevant and not excessive for any particular purpose;
4. must be accurate and kept up to date;
5. not kept for longer than is necessary;
6. processed in accordance with rights of data subjects for personal data;
7. secure and protected to prevent unlawful or unauthorised processing, accidental loss, destruction or damage;
8. not transferred to countries outside EEA (European Economic Area) without adequate protection.

Note that the Data Protection Act is not restricted to information held on computer, but also covers information held in other media such as paper and microfiche.

The Society's Data Protection Notification is available on the ICO website:
<http://www.ico.gov.uk/ESDWebPages/search.asp> under registration number
Z5958155

1. General Provisions

1.1 The stated reasons registered with the ICO for the Society holding personal data are as follows:

- to administer and maintain Membership records;
- to respond to any query raised about Membership records;
- as input to a code of conduct complaint;
- to administer and maintain employees' records;
- to keep members informed about products or services the Society or approved 3rd parties can offer;
- use information about the member for the purposes of research and statistical analysis;
- disclose information about members to regulatory authorities in response to formal requests.

2. Data subject scope

2.1 The Categories of Data Subjects for the Society are as follows:

- Current, past, and potential members
- Current, past, and potential non-members
- Current, past and potential employees
- Current and past non-Society members of website services

3. Principals

3.1 Data shall not be processed unless the Data subject has given consent, or processing is necessary for (primarily) performance of contract, compliance with legal obligation, or administration of justice.

3.2 Exemptions to all or some of the Principles include confidential references, aspects of examinations work (separate Guideline), and legal professional privilege

4. Policy and procedure

4.1 The Society can legally disclose some member data under specific circumstances. For example, the Society publishes a number of searchable lists on the main website that can be accessed by members and the public. As this data is in the public domain and members have opted into appearing on such lists, it is acceptable to give out this data to enquirers provided it will be used for the same reason the data was originally captured.

Therefore, data appearing on the Directory of Chartered Psychologists can be given over the telephone to a member of the public seeking the services of a psychologist.

4.2 Data sets

4.2.1 The Society holds two main address data sets. The Main Address (appearing on the left hand side of the database screen) is used for Society mailings, and is not used for any publically-accessible list or communication with any third parties unless legally required to do so. Therefore address data in these fields should never be given out to enquirers.

4.2.2 The second data set is labelled Public Register Address. For Chartered Psychologists it is this data set that appears on the mandatory and publically-accessible List of Chartered Members searchable list. Data appearing in these fields for Chartered Members can be given out to enquirers, unless the member has opted out of all public lists as indicated by the 'Do Not Give out Address' message displayed when accessing the member record in the Stratum database.

4.3 Enquirer validation

4.3.1 Staff must validate personal details with any telephone enquirer to ensure they are speaking to the actual member or someone correctly acting on behalf of the member. This is done by asking the enquirer to confirm specific personal details on the member record:

- Full Name
- Membership Number
- Date Of Birth

Then one from the following:

- Mailing Address Postcode
- First Line Of Mailing Address
- Email Address used to communicate with the member regarding membership matters

4.4 Subject access right requests

4.4.1 Anyone for whom the Society holds data can request to see the data the Society holds for them. These are called Subject Access Requests.

4.4.2 Subject Access Requests will only be accepted from the person whose data is being requested, except where a certified legal request is received.

4.4.3 All requests received are to be passed to the Society's Data Protection Officer for action. In producing the response the following areas will need to be covered:

- a description of why the information is processed;

- any external company / third party it may have been passed to or seen by;
 - logic involved in any automated decisions such as automatic publishing on searchable lists;
- 4.4.4 The format of response must be easy to understand and any codes should be explained.
- 4.4.5 A response to a Subject Access Request will be:
- In printed format only
 - Not de-duplicated
 - Redacted if containing DPA data of other parties
 - In non-chronological order
- 4.4.6 Searches for subject data includes all electronic and structured manual data sources.
- 4.4.7 A fee of £10 is charged for full Subject Access Requests (a fee that is legally restricted) and the response will be provided within 40 calendar days.
- 4.4.8 Partial access requests (e.g. a request for a copy of an individual form or piece of correspondence) may be accepted and processed free of charge at the discretion of the Society's Data Protection Officer.

5. Non-compliance consequences

- 5.1 Any breaches of the Data Protection Act can lead to one or more consequences:
- Civil action by an aggrieved individual
 - Enforcement notice and possible fine on the Society
 - Criminal offence
 - Adverse publicity for the Society
 - Disciplinary action

For any further queries and questions on the Data Protection Act 1998 contact the Society's Data Protection Offices (Director of Corporate Services).