GPTI Data Protection Policy

The following is the policy of GPTI regarding handling of data. This policy applies to GPTI and all of its constituent committees, boards and subsidiary organisations

The Principles

GPTI shall:

1 Process personal data fairly and lawfully and, in particular, not process data unless these principles and the rules set out here are followed.

2 Obtain personal data only for specified and lawful purposes, and not process data in any manner incompatible with that purpose or those purposes.

3 Obtain personal data that is adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4 Keep personal data accurate and up to date.

5 Not keep personal data for longer than is necessary for their legitimate purposes.

6 Process personal data in accordance with the rights of data subjects under the Data Protection Act.

7 Take appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8 Not transfer personal data to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

What is Data Protection?

The Data Protection Act (the Act) aims to protect individual's fundamental rights and freedoms, notably privacy rights, in respect of personal data processing.

The Act applies to paper and electronic records held in structured filing systems containing personal data, meaning data which relates to living individuals who can be identified from the data.

Data protection operates by giving individuals the right to gain access to their personal data. This is done by making a subject access request in which they are entitled to:

- a description of their personal data
- the purposes for which they are being processed
- details of whom they are or may be disclosed to

Individuals can also prevent processing of their data in certain circumstances, opt-out of having their data used for direct marketing and in automated decision making processes,

apply to the courts for inaccurate data to be corrected and claim compensation for damage and distress caused as a result of any data protection breach.

All organisations must notify the Information Commissioner of the processing of personal data; this is included in a public register. The public register of data controllers is available on the Information Commissioner's website (http://www.ico.gov.uk/), from where you can search for GPTI's or any other organisation's notification.

Data Subjects
Data Subjects are defined as being individuals about whom information is held.

- Psychotherapists
- Trainees
- Complainants, correspondents and enquirers
- Advisors, consultants and other professional experts

Data Classes
Data classes are the types of data which are being or which are to be processed:

- Personal Details
- Education and Training Details
- Employment Details
- Offences (including alleged offences)
- Criminal proceedings, outcomes and sentences
- Financial details
- Goods or services provided

Recipients
Recipients are individuals or Organisations to whom GPTI as a data controller intends or may wish to disclose data. This list does not include any person to whom the GPTI as a data controller may be required by law to disclose in any particular case, for example if required by the police under a warrant.

This list should not be read as a list of those to whom data ***will*** be disclosed. GPTI is required to make clear all of the possible categories of 'recipient' to which they might need or wish to disclose data – either in pursuit of their regulatory and public protection functions or in relation to permissions sought from and granted by a data subject.

- Data subjects themselves
- Current, past or future employers
- Healthcare, social and welfare advisors or practitioners
- Education, training and accrediting establishments and examining bodies
- Employees and agents of GPTI
- Suppliers, providers of goods and services
- Persons making an enquiry or complaint
- Police forces
- Private investigators
- Local government
- Central government
- Voluntary and charitable organisations
- Ombudsmen and regulatory authorities

Purposes
The purposes to which GPTI as a Data Controller may put the data held are described here. This list does not represent the purposes to which all data held will always be put to.

GPTI holds a wide range of data types relating to diverse data subjects. At various times the data held in respect of these subjects may be used in relation to some or all of the following purposes:

Accounting and auditing
The provision of accounting and related services; the provision of an audit where such an audit is required by statute.

Administration of complaints processes
The administration of complaint and grievance processes of all kinds, including professional disciplinary processes, and complaints against officers, committees or other subsidiary bodies.

Administration of membership records
The administration of membership records.

Education
The provision of education, training, accreditation and reaccreditation, supervision and/or research as a primary function or business activity.

Information and databank administration
Maintenance of information or databanks as a reference tool or general resource. This includes catalogues, lists, directories and bibliographic databases.

Licensing and registration
The administration of licensing or maintenance of official registers.

Processing for *not for profit* organisations
Establishing or maintaining membership of or support for a body or association which is not established or conducted for profit, or providing or administering activities for individuals who are either members of the body or association or have regular contact with it.

Realising the objectives of a voluntary body
The provision of goods and services in order to realise the objectives of the voluntary body.

Individual Member Consent
In order to be registered with the GPTI, members must agree to GPTI holding the required details (along with any additional optional information requested that they elect to supply) and information on our computer Database. If members do not agree to this they cannot be entered on the GPTI register. GPTI undertakes to use the information that members provide in accordance with the Data Protection Act and GPTI policies. GPTI is a registered Data Controller under the Data Protection Act 1998 and follows data protection guidelines in relation to all use and storage of data held by them.

For GPTI to effectively perform its function it is necessary, at times, to send information to member. By registering with GPTI, members agree that GPTI may use their contact details to correspond with them.

Duration of Data Retention
As a data controller GPTI must not hold data for longer than required or after the data subject's relationship with the GPTI has been terminated.

Sensitive Data
GPTI does not collect sensitive data except that criminal records are required to be disclosed to the Ethics Committee: Sensitive data consists of racial/ethnic origin, political opinions, religious beliefs, membership of trade union, physical/mental health, sexual orientation, criminal records.

Security
GPTI operates in a field in which confidentiality and record security is of paramount importance. GPTI's office is operated on the basis that all material entering the office be regarded as confidential until otherwise defined.

Subject Access
Please email the administrator on admin@gpti.or.uk for a record of data held and this will be provided within one month.

Data breach
A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.

The relevant supervisory authority will be notified of a breach where it is likely to result in a risk to the rights and freedoms of individuals. If unaddressed such a breach is likely to have a significant detrimental effect on individuals – for example, result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

What information must a breach notification contain?

The nature of the personal data breach including, where possible:

- the categories and approximate number of individuals concerned; and
- the categories and approximate number of personal data records concerned;
- A description of the likely consequences of the personal data breach; and
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.

Review of this Policy

This policy shall be reviewed annually by the Executive Council