# The Site for Contemporary Psychoanalysis Data Protection Policy

## Introduction

Given the inherently sensitive nature of psychoanalytic work, the responsible handling of data is of paramount importance. The commitment to patient confidentiality and ethical responsibility extends into all spheres of operation for a psychoanalytic training organisation. The aim of this Data Protection Policy is to provide comprehensive guidelines regarding the collection, storage, use, and disposal of data, in compliance with Data Protection Act 2018 and other local data protection laws.

The Site is committed to protecting the rights and freedoms of all individuals in relation to the processing of their personal data and provides this Data Protection Policy for everyone to follow.

## The Scope of this Policy

We need to comply with the Data Protection Act (as amended from time to time) in relation to all personal data that is processed by the Site. To ensure this happens, we have developed this policy which sets out the obligations of the Site in this respect.

This policy and the Data Protection Act apply to all personal data handled by the Site, both that held in paper files and data held electronically. So long as the processing of the data is carried out for Site purposes, it also applies regardless of where data is held, (for example, it covers data held at our office and on mobile devices such as electronic notebooks or laptops) and regardless of who owns the PC/device on which it is stored.

'Processing' data is widely defined and includes every plausible form of action that could be taken in relation to the data such as obtaining, recording and keeping, or using it in any way; sharing or disclosing it; erasing and destroying it.

## Definitions

### Personal data

Data which relates to a living individual who can be identified from that data and other information which is in the possession of, or is likely to come into the possession of, the data controller. The Site is the data controller.

Examples of personal data are the name and address of any individual, a member or trainee which when put with other information held by the Site could identify that member or trainee.

## Data Subject Rights

An individual's rights (all of which are qualified in different ways) are as follows:

- the right to be informed of how their personal data are being used. This right is usually fulfilled by the provision of 'privacy notices' (also known as 'data protection statements' or, especially in the context of websites, 'privacy policies') which set out how an organisation plans to use an individual's personal data, who it will be shared with, ways to complain, and so on;
- the right of access to their personal data;
- the right to have their inaccurate personal data rectified;
- the right to have their personal data erased (right to be forgotten);
- the right to restrict the processing of their personal data pending its verification or correction;
- the right to receive copies of their personal data in a machine-readable and commonly-used format (right to data portability);
- the right to object: to processing (including profiling) of their data that proceeds under particular legal bases; to direct marketing; and to processing of their data for research purposes where that research is not in the public interest;
- the right not to be subject to a decision based solely on automated decision-making using their personal data.

Special Category Data (previously called Sensitive Personal Data)

Some personal data are more sensitive in nature and therefore requires a higher level of protection. The legislation refers to the processing of certain data as 'special categories of personal data'. This means personal data about an individual's:

race or ethnic origin of the data subject
their political opinions
their religious beliefs or philosophical beliefs whether they are a member of a trade union
their physical or mental health or condition
their sexual life
sexual orientation
biometric data (where this is used for identification purposes)
any commission or alleged commission by them of any offence any proceeding
for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.

Committee members or the administrators working in certain areas (e.g. membership committee, training committee, ethics committee) may have regular access to special category data.

## Confidential data

Data given in confidence or data agreed to be kept confidential (in other words, a secret between two parties) and that is not in the public domain.

Some confidential data will also be personal data and/or sensitive personal data and therefore come within the terms of this policy. Committee members or the administrator working in certain functions and in senior roles will handle confidential data regularly.

## Legal Framework

The Site needs to collect and keep certain types of information about the people with whom it deals. This includes information relating to its members and trainees and other individuals. It needs to process 'personal data' for a variety of reasons, such as to record the academic progress of its trainees, the engagement of teaching faculty members and to comply with statutory obligations (for example, health and safety requirements).

The Data Protection Act applies to all 'personal data' processed by the Site and to comply with the law all personal data must be collected and used fairly, stored safely and not disclosed to anyone else unlawfully. As part of this, The Site must have a 'legal basis' for processing an individual's personal data (most commonly, the processing is necessary for The Site to operate a contract with them, the processing is necessary to fulfil a legal obligation, the processing is in the legitimate interests of The Site and does not override their privacy considerations, or they have consented to the processing)."

## Responsibilities of committee members, administrators and trainees

All committee members, administrators and trainees must:

Be mindful of the fact that individuals have the right to see their 'personal data' (and this may include for example information received from prospective trainees written in connection with an application to the Site or any comments written about them in emails). They should not, therefore, record comments or other data about individuals which they would not be comfortable with the individual seeing, either in emails or elsewhere.

Immediately report to the chair of the Site and bring it to the attention of the Data Protection Officer, if they find any lost or discarded data which they believe contains personal data, (for example, may include a memory stick).

Immediately report to the chair of the Site and bring it to the attention of the Data Protection Officer, if they become aware that personal data has been accidentally lost or stolen or inadvertently disclosed (for example, if their laptop is stolen or their phone is lost and it has personal data stored on it),

Hold the contents of any personal data which comes into their possession securely.

Ensure that any personal data they provide to the Site (for example, their contact details) is accurate.

Notify the Site promptly of any changes to their personal data (for example, change of address or emergency contact details).

Only ever obtain or use personal data relating to third parties for approved work or study-related purposes.

Committee members, administrators and trainees who process 'personal data' must:

Ensure that they only ever process personal data in accordance with requirements of the Data Protection Act and in particular: ensure that they have a valid lawful basis in order to process the data before commencing the processing; and only process 'special category data', if the processing meets one of the additional conditions for special category data; and follow the 6 Data Protection principles. The best way to ensure compliance is through familiarisation with this policy and the guidance we provide. Key points insofar as compliance is concerned include:
Fair processing - for example, ensure that the individual consents to their data being used and knows what it will be used for, and ensure that it is not subsequently used for something else.

Data Security - ensure any personal data which is held is always kept and disposed of securely, (taking into account any cybersecurity considerations).

Non-disclosure - ensure personal data is not disclosed to any unauthorised third party.

Familiarise themselves with the guidance and other information published by the Site and follow it at all times.

Be mindful of the scope of Data Protection regulations. This includes that fact that 'personal data' is widely defined, (and so will cover for example comments made about an individual in an email to someone else), and the fact that it covers data held on remote devices (such as tablets and on mobile phones) regardless of who owns the actual device and where the device is stored.

Seek advice whenever a new or novel form of processing personal data is contemplated or if any data protection related concerns ever arise.

## Personal data in the public domain

We hold certain information about members, administrators and trainees in the public domain. Personal data classified as being in the 'public domain' refers to information which will be publicly available worldwide and may be disclosed to third parties without recourse to the data subject.

Our practice is to make the following items of data freely available unless individuals have objected:

names of members of Council
members, administrators workplace email addresses and telephone numbers
teaching facultiy members biographies and curricula vitae where supplied
names and academic qualifications of teaching faculty members where appropriate
any additional information relating to data subjects which they have agreed to be placed in the public domain and which may be in automated and/or manual form.

Similarly, as part of its regular business activities, the Site may process personal information about third parties which is already in the public domain where such processing is carried out in accordance with the Data Protection Act principles set out below and is unlikely to cause any damage or distress to the data subject.

## Data Protection Act principles

Anyone using personal data must comply with the 6 Data Protection Principles contained in the Data Protection Act 2018 as they define how personal data can be legally processed: In summary these state that personal data shall:

Be obtained and processed fairly, lawfully and transparently.
Be processed for specified explicit and lawful purposes and shall not be processed in any manner incompatible with these purposes.
Be adequate, relevant and not excessive for those purposes.
Be accurate and kept up to date.
Not be kept for any longer than is necessary.
Be processed in a secure manner.

## Data security

Keeping personal data properly secure is key in complying with the Data Protection Act. All committee members and administrators are therefore responsible for

ensuring that if they keep personal data, it is kept securely and is not disclosed (either orally or in writing or accidentally) to any unauthorised party.

This includes, as a minimum:

Ensuring that any personal data recorded in paper form or hard copy documents are kept in locked filing cabinets or locked drawers or in locked offices.

Ensuring that the same measures are taken in regards to any discs or memory sticks or similar devices on which personal data is held, for example, they must also be kept in a secure and locked location.

Ensure that if any personal data is held on a Mobile Device that it is properly password protected and where appropriate encrypted.

Ensuring special care is taken whenever data is transferred from one place to another to ensure the security of the data is paramount, (for example, to avoid losing memory sticks in transit or to avoid sensitive personal data being transferred to a PC which is not password protected and encrypted).

## Data Retention and Timescales

Administrative Data: Kept for a period of 7 years after the end of administrative utility.

Student Records: Maintained for 10 years after the completion or the termination of training.

Financial Records: Preserved for 7 years for tax and auditing purposes.

Ethics and Complaint Records: Stored for 10 years after resolution.

## Prohibited activities.

The following activities are strictly prohibited:

Using data obtained for one purpose for another supplemental purpose (for example, using contact details provided for training related purposes for marketing purposes)
Disclosing personal data to a third person outside the Site without the consent of the data subject.

## Right to access information

Individuals have the right to access any personal data that relates to them which the Site holds. Any person who wishes to exercise this right should contact the data controller in writing

## Implications of breaching this policy

It is a condition of enrolment in the case of trainees or membership in the case of members that trainees and members will abide by the policies and rules of the Site. Any breach of this policy will be considered to be a disciplinary offence and may lead to disciplinary action. A serious breach of the Data Protection Act may also result in the Site and/or the individual being held liable in law.

### Accountability

The Site is required under law to:

- comply with data protection law and hold records demonstrating this;
- implement policies, procedures, processes and training to promote "data protection by design and by default";
- have appropriate contracts in place when outsourcing functions that involve the processing of personal data;
- maintain records of the data processing that is carried out across The Site;
- record and report personal data breaches;
- carry out, where relevant, data protection impact assessment on high risk processing activities;
- cooperate with the Information Commissioner's Office (ICO) as the UK regulator of data protection law;
- respond to regulatory/court action and pay administrative levies and fines issued by the ICO.

## Conclusion

Compliance with the Data Protection Act is the responsibility of all members of the Site, administrators and trainees. Any questions about this policy or any queries concerning data protection matters should be raised with the Data Protection Officer.