IPSS Data Protection Policy. (29/04/2019)

The following is the policy of IPSS regarding handling of data. This policy applies to IPSS and all of its constituent committees. IPSS Members are required to adopt data protection policies consistent with this Policy. The term “member” in this document refers to all IPSS members.

The Principles

IPSS 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.
9. All IPSS Members and Membership Applicants have the right to request information about their personal data held by IPSS.

Action taken by IPSS to comply with these principles:

- IPSS is registered with The Information Commissioner’s Office, (ICO) and renews its registration annually.
- IPSS has introduced a data protection policy and any breach of that policy is taken seriously and addressed.
- IPSS is committed to take action to maintain that all personal data held on members and their clients is kept private and confidential.
- The majority of IPSS Member information passes through the Administrator is stored in her computer and is directly accessible to her alone.
- All Personal Data from Members' annual application forms are stored on the administrator's PC.
- Personal Data from Applications for Membership, Late membership renewal, Applications for Accreditation and 5 Yearly Re-accreditation submissions are shared with Council and delegated Committee Members by email as required and stored on their personal computers while the applications are considered.
- That data will be held on Council and delegated Committee Members' Computers, Phones or other IT devices no longer than required.
- IPSS Council reviews the amount of data held by the Administrator and Council and Committee Members, every 4 months at Council to ensure that no personal data is held on members or their clients, longer than is required.
- IPSS as an UKCP Member Organisation requires that its members take both the necessary and timely steps in complying with data protection requirements in their own professional practice.