

DATA PROTECTION POLICY

Addressing the General Data Protection Regulation (GDPR) 2016 (EU) and the Data Protection Act (DPA) 2018 (UK)

Definitions

Property People's Network (PPN) holds personal data about its employees, members, suppliers and other individuals for a variety of business purposes. This policy sets out how PPN seeks to protect personal data and ensure that all Committee Members of the Organisation understand the rules governing the use of personal data to which they have access in the course of their work.

Business purposes:

The purposes for which personal data may be used by PPN: membership management, event administration and management of subscriptions.

Business purposes include the following:

- Compliance with PPN's legal and governance obligations and good practice
- Ensuring privacy policies are adhered to (such as covering email and internet use)
- Operational reasons, such as recording transactions, event planning and bookings, distribution of information and merchandise
- Investigating complaints
- Checking references, ensuring safe working practices, monitoring and managing Committee Member access to administrative information
- Promoting PPN
- Improving services to members

Personal data:

Information relating to identifiable individuals, such as new applicants, current and former members, other Committee Members, suppliers and other PPN contacts.

Personal data PPN gathers may include: individuals' contact details and subscription details.

Sensitive personal data:

Personal data about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings **is not requested, sought or held by PPN.**

A member may request to look at the information PPN holds on her/him.

Scope

This policy applies to all Committee Members who must be familiar with this policy and comply with its terms.

This policy may be supplemented or amended by additional policies from time to time.

This Policy is agreed by PPN Committee members who are responsible for its implementation.

Our procedures:

Fair and lawful processing

PPN must process personal data fairly and lawfully in accordance with individual's rights.

The Data Controller's Responsibilities

- Keeping the Committee updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and policies on a regular basis
- Arranging data protection guidance and advice for all Committee Members
- Answering questions on data protection from Members and Suppliers who wish to know what data is being held on them by PPN
- Checking and approving with third parties that handle PPN's data, any contracts or agreement regarding data processing such as IT providers and Caterers

Additional responsibilities of the Secretary

- Ensure all systems, services, software and equipment meet acceptable security standards
- Checking and scanning security hardware and software regularly to ensure it is functioning properly
- Researching third party services, such as cloud services PPN is considering using to store or process data
- Approving data protection statements attached to emails and event notices

The processing of all data must be:

- Necessary to deliver services to our members
- In PPN's legitimate interests and not unduly prejudice the individual's privacy.

In most cases this provision will apply to routine Membership and Event data processing activities.

PPN will send out a Privacy Notice to Members on data protection.

This notice:

- Sets out the purposes for which we hold personal data on Members
- Highlights that PPN's work may require us to give information to third parties such as event venues and catering companies
- Provides that customers have a right of access to the personal data that is held about them.

Accuracy and relevance

PPN will ensure that any personal data it processes is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. PPN will not process personal data obtained for one purpose for any unconnected purpose, unless the individual concerned has agreed to this or would otherwise reasonably expect it.

Individuals may ask that PPN correct inaccurate personal data relating to them. If a member believes that information is inaccurate they should record the fact that the accuracy of the information is disputed and inform the Secretary.

Your personal data

Each member must take reasonable steps to ensure that personal data PPN holds about them is accurate and updated as required. For example, if personal circumstances change, please inform the Secretary so that the data can be updated in the records.

Data security

PPN must keep personal data secure against loss or misuse. Where other organisations process personal data as a service on PPN's behalf, the Secretary will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third-party organisations.

Storing data securely

- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it
- Printed data should be shredded when it is no longer needed
- Data stored on computer should be protected by strong passwords that are changed regularly
- Data stored on CDs or memory sticks must be locked away securely when they are not being used
- The Secretary must approve any cloud service used to store data
- Any servers containing personal data must be kept in a secure location, away from general office space
- Data should be regularly backed up in line with PPN's backup procedures
- Unless authorised, data should not be saved directly to mobile devices such as tablets or smartphones
- All servers containing sensitive data must be approved and protected by security software and a strong firewall.

Data retention

PPN must not retain personal data for longer than is necessary. Members who do not renew their membership within 6 months of expiry will have their details removed from the PPN website and records.

Subject access requests

Under the Data Protection Act 1998, individuals are entitled, subject to certain exceptions, to request access to information held about them. This requirement is included in the GDPR 2018 and is expected to be included in the DPA 2018.

Subject access requests from Members or Committee Members should be referred immediately to the Secretary.

Processing data in accordance with individual's rights

PPN will abide by any request from an individual not to use their personal data for direct marketing purposes and notify the Secretary about any such request.

PPN will not send direct marketing material to someone electronically unless we have an existing business relationship with them in relation to the services being marketed.

Training

The Secretary has received training on this policy covering:

- The law relating to data protection
- Our data protection and related policies and procedures.

Further training will be obtained whenever there is a substantial change in law or our policy and procedure.

GDPR 2018 provisions

Where not specified previously in this policy, the following provisions will be in effect on or before 25 May 2018.

Privacy Notice – transparency of data protection

Being transparent and providing accessible information to individuals about how we use members' personal data is important to PPN. The following are details on how PPN collects data and what PPN will do with it:

What information is being collected?	<p><u>Membership Information:</u> Full name, address, telephone and email contacts, subscription and event payment details, professional experience/aspirations to join the Committee or interests as they relate to PPN activities.</p> <p><u>Event Information:</u> Participants attending events may be asked for dietary requirements and for permission of any photographs in which they appear to be included on the PPN website Gallery and/or PPN Newsletter.</p>
Who is collecting it?	The Secretary
How is it collected?	Application forms/email/event booking forms and is stored digitally and/or on hard copy.
Why is it collected?	To process applications, arrange admissions, establish accurate event arrangements.
How will it be used?	Maintain a database, generate address labels and letters, book event numbers and request dietary requirements. To notify members of PPN events, make event arrangements, update members on PPN matters and to notify members of subscription renewals.
Who will it be shared with?	<ul style="list-style-type: none">• Within PPN, the Secretary and Committee Members. Outside PPN with relevant academic institutions with members' permission and where subscription fees are paid by a third party, ie, university or employer. PPN's work may require us to give information to third parties such as event venues and catering companies.

Identity and contact details of any data processors	The Secretary. Email: ppnsecretary@outlook.com
Details of transfers to third country and safeguards	Not applicable.
Retention period	Names, contact details and relevant PPN admission data, resignation and death dates are maintained in the database as a historical record of PPN members for 6 months after the date of membership expiry.

Conditions for processing

PPN will ensure any use of personal data is justified using at least one of the conditions for processing and this will be consent. All Committee Members who are responsible for processing personal data will be aware of the conditions for processing. The conditions for processing will be available to data subjects in the form of a privacy notice.

Justification for personal data

PPN will process personal data in compliance with all six data protection principles.

Consent

The data collected is subject to active consent by the data subject. This consent can be revoked at any time.

Data portability

Upon request, a data subject should have the right to receive a copy of their data in a structured format. These requests should be processed within one month, provided there is no undue burden and it does not compromise the privacy of other individuals. A data subject may also request that their data is transferred directly to another system. This must be done for free.

Right to be forgotten

A data subject may request that any information held on them is deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies.

Privacy by design and default

Privacy by design is an approach to projects that promote privacy and data protection compliance from the start. The Secretary will be responsible for conducting Privacy Impact Assessments and ensuring that all IT projects commence with a privacy plan. When relevant, and when it does not have a negative impact on the data subject, privacy settings will be set to the most private by default.

International data transfers

PPN does not transfer data outside the UK.

Data audit and register

Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

Reporting breaches

All Committee Members have an obligation to report actual or potential data protection compliance failures. This allows PPN to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the Information Commissioner's Office (ICO) of any compliance failures that are material either in their own right or as part of a pattern of failures

Monitoring

Everyone must observe this policy. The Secretary has overall responsibility for this policy and will monitor it regularly.

Consequences of failing to comply

PPN takes compliance with this policy very seriously. Failure to comply puts both you and PPN at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action.

If you have any questions or concerns about this policy, contact the Secretary.

David Ross
Chair PPN

April 2018