Data protection policy and General Data Protection Regulations (GDPR) compliance

This is a statement of the data protection policy adopted by Practice 2 Practice Ltd.

We will be reviewing and updating this privacy statement in line with the new General Data Protection

Regulation (GDPR) requirements which are effective from 25 May 2018.

The management team are fully aware of the requirements of GDPR and are engaged in a full review of our systems and third-party software providers to ensure that we comply with the requirements, and remain so beyond the effective date.

Up to the effective date we remain registered with the Information Commissioner and comply with current regulations. In order to carry out our work, we may need to collect and use certain types of personal information about the people we deal with, such as current, past and prospective employees, students, suppliers, clients, professional contacts and others with whom we communicate.

In addition, we may occasionally be required by law to collect and use certain types of personal information in order to comply with the requirements of government departments and agencies.

Under the Data Protection Legislation, all organisations which handle personal information must comply with a number of important principles regarding the privacy and disclosure of this information. We are committed to compliance with these principles.

We believe that the lawful and correct treatment of personal information is critical to our successful operation, and to maintaining the confidence of our stakeholders in us. We recognise that, to maintain our reputation and integrity as an open and professional organisation, we must be fully compliant with this legislation.

Data Protection Legislation

In the United Kingdom and the European Economic Area (EEA), "Data Protection Legislation" means all applicable data protection and privacy legislation or regulations including The Privacy and Electronic Communications (EC Directive) Regulations 2003 (also known as PECR) and any guidance or codes of practice issued by the European Data Protection Board or the Information Commissioner, together with:

- prior to 25 May 2018, the UK Data Protection Act 1998; and
- from 25 May 2018 onwards Regulation (EU) 2016/679 (the "General Data Protection Regulation" or "GDPR"), as amended by the UK Data Protection Bill.

Outside of the EEA, "Data Protection Legislation" means local, territorial data protection and privacy legislation that governs the processing of Personal Data.

We fully endorse and adhere to the principles of data protection set out in the Data Protection Legislation and will:

- fully observe the conditions regarding the fair collection and use of personal information;

- meet our legal obligations to specify the purposes for which we use personal information;
- only collect and process the personal information needed to carry out our business or to comply with any legal requirements;
- ensure that the personal information we use is as accurate as possible;
- ensure that we don't hold personal information any longer than is necessary;
- ensure that people know about their rights to see the personal information we hold about them;
- take appropriate technical and organisational security measures to safeguard personal
- information; and
- ensure that personal information is not transferred abroad without suitable safeguards.

As part of our GDPR review, we will be reviewing our systems, data processes and procedures to identify how we manage personal data – how we got it, who can access it, where it is stored and how long it should be kept.

We will also be addressing key areas including breach reporting, subject access and data retention so that you can ensure your data is safe with us.

With regards to individuals, we recognise the following rights under GDPR:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure;
- the right to restrict processing;
- the right to data portability;
- the right to object; and
- the right not to be subject to automated decision-making including profiling.

In addition, we will ensure that:

- there is someone with specific responsibility for data protection in the organisation. Currently, the nominated person is Compliance Officer Mike Couzens; email mike@p-2-p.co.uk
- we regularly review and audit how we handle personal information;
- the ways we handle personal information are clearly described;
- everyone handling personal information understands that they are responsible for following
- good practice;
- everyone handling personal information is appropriately trained and properly supervised;
- we regularly assess the performance of people who handle personal information;
- anybody wanting to make enquiries about handling personal information knows what to do; and
- queries about handling personal information are deal with promptly and courteously.

You have the right to request a copy of the personal information that we hold about you. To do so please write to Practice 2 Practice Ltd, 3rd Floor, 3 Brindleyplace, Birmingham B1 2JB

We charge a fee for this service, which will be dependent on the required level of data requested.

Specific GDPR requirement as a 'data processor'

There are specific responsibilities under GDPR that provide sufficient guarantees that the requirement of the GDPR will be met and the rights of the data subjects protected.

We provide the following:

- As processors we only act on written instructions of the controller (unless required by law to act without such instruction)
- We ensure that people processing the data are subject to a duty of confidence
- We take appropriate measures to ensure the security of processing. To this end we use 256k Secure Socket Layer (SSL) encryption technology in conjunction with password protected databases.
- We look to assist the data controller in providing subject access and allowing data subjects to exercise their rights under GDPR
- We look to assist the data controller in meeting it's GDPR obligations in relation to the security pf processing, notification of personal data breaches and data protection impact assessments
- We will delete or return all personal data to the controller as requested at the end or during the termination period of any contract
- All processing of data takes place within the EU on EU compliant servers

GDPR checklist

- We have documented the subject matter of our data processing procedures
- We have documented the duration of our data processing procedures
- We have documented the type of data that we process
- We have documented the categories of data subject and obligations there of

Approved March 2018.