INFORMATION MANAGEMENT POLICY

KPM has a policy for the overall management of all electronic data. The responsibility for its management is with Karen South. This policy is reviewed annually by the Partners as part of its Lexcel annual review process.

KPM holds the following categories of data which are classified as information assets and client data:

1. Staff Administration

    1.1 Personal details;
    1.2 Family, lifestyle & social circumstances;
    1.3 Education & training details;
    1.4 Employment details;
    1.5 Financial details;
    1.6 Racial or ethnic origin;
    1.7 Religious or other beliefs of a similar nature;
    1.8 Trade Union membership;
    1.9 Physical or mental health or condition.

2. Advertising, Marketing & Public Relations

    2.1 Personal details;
    2.2 Family, lifestyle & social circumstances;
    2.3 Goods or services provided.

3. Accounts & Records:

    3.1 Personal details;
    3.2 Financial details;
    3.3 Goods of services provided.

4. Legal Services:

    4.1 Personal details;
    4.2 Family, lifestyle & social circumstances;
    4.3 Education & training details;
    4.4 Employment details;
    4.5 Financial details;
    4.6 Goods or services provided;
    4.7 Racial or ethnic origin;
    4.8 Political opinions;
    4.9 Religious or other beliefs of a similar nature;
    4.10 Trade Union membership;
    4.11 Physical or mental health or condition;
    4.12 Sexual life;
    4.13 Offences (including alleged offences);
    4.14 Criminal proceedings, outcomes & sentences.

KPM has identified the following critical risk(s) to the data specified above:

- Insufficiently robust systems for safeguarding confidentiality and other information assets of the practice.
- Insufficient controls to identify inappropriate e-mails.
- Insufficient controls to identify misuse of the Internet.
- Ensuring there is a system in place to register and renew with the Information Commissioner by the correct date.
- Lack of staff knowledge of the principles of the Data Protection Act 1988.

KPM has in place the following processes, procedures and technology to eliminate, minimise or transfer the critical risks identified above:

- Initiation of update training in data protection and information management procedures.
- Constant upgrade and review of IT security software.
- Introduction of periodic IT security audits.

KPM provides periodical training to all staff as follows:

- Fee Earners – amass annual CPD points.
- Support staff – tailored packages to suit ongoing training needs throughout KPM's financial year.

Management of KPM's electronic document technology is the responsibility of Jason Jackson of Apnet Limited of Compass House, 36 East Street, Bromley, Kent, BR1 1QU.

The types of document to be held in the systems for managing documents are:

- Practice documents (leases, etc.);
- Client documents (agreements, court orders, etc.);
- Staff documents (contracts, etc.);
- Others (as required).

KPM has in place the following procedures, and operates the following technologies, for safeguarding the integrity of electronic documents:

- Documents are stored on a central server and the contents of the server are backed up on every work night to a tape that is taken offsite the following day; and
- Archived documents are stored onto disk offsite by Microeye Services Limited of Howbury House, Thames Road, Crayford, Dartford, Kent, DA1 4RQ, who will also arrange for the retrieval of archived documents.

Subject Access Requests

Any individual whose data is held by KPM may make what is called a 'subject access request', i.e. a request to see what data is actually held about them. All such requests should be addressed in writing to Karen South and she will arrange for KPM to comply promptly with the request in accordance with the disclosure requirements of the Data Protection Act.