THE LAW SOCIETY OF NORTHERN IRELAND

DATA PROTECTION POLICY

1. Introduction

1.1 Everyone has rights with regards to how their personal information is handled. During the course of our activities we will collect, store and process personal information about our staff, solicitors and other living individuals. We recognise the need to treat this information in an appropriate and lawful manner.

1.2 The types of information that we may be required to handle include details of current, past and prospective employees, members of the solicitors profession, their clients and others with whom we communicate.

1.3 The information, which may be held on paper or on a computer or other media is subject to certain legal safe guards specified in the Data Protection Act 1998 (the Act) and other regulations. The Act imposes restrictions on how we may use that information.

2. Status of the Policy

2.1 This Policy has been approved by the Council of the Law Society of Northern Ireland. It sets out our rules on data protection and the legal conditions that must be satisfied in relation to the obtaining, handling processes, storage, transportation and destruction of personal information.

2.2 The Society's Data Protection Officer is Peter O'Brien, Deputy Secretary, Law Society of Northern Ireland, 96 Victoria Street, Belfast BT1 3GN who is responsible for ensuring compliance with the Act and this Policy.

2.3 If you consider that this Policy has not been followed in respect of personal information about yourself or others, you should raise the matter with the Data Protection Officer.

2.4 This Policy should be read in conjunction with our Privacy Notice which gives further guidance on how the Law Society processes information.

3. Definition of data protection terms

3.1 Data is information which is stored electronically on a computer or in certain paper based filing systems;

3.2 Data subjects for the purpose of this Policy include all living individuals about whom we hold personal information. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.

3.3 Personal information means information relating to a living individual who can be identified from that information (or from that information and other information in our possession). Personal information can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal).

3.4 Data controllers are the people within our organisation who determine the purpose for which and the manner in which any personal information is processed. They have a responsibility to establish practices and policies in line with the Act.

3.5 Data users include employees whose work involves using personal information. Data users have a duty to protect the information that they handle by following our data protection and security policies at all times.

3.6 Data processors include any person who processes personal information on behalf of a data controller.

3.7 Processing is any activity that involves the use of information. It includes obtaining, recording or holding information or carrying out any operation or set of operations on the information including organising, amending, retrieving, using, disclosing, erasing, or destroying it.

3.8 Sensitive personal information includes the information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life or about the commission of or proceedings for any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal information can only be processed under strict conditions and will usually require the consent of the person concerned.

4. Data protection principles

4.1 Anyone processing personal information within the Law Society must comply with the eight enforceable principles of good practice. These provide that personal information must be:-

(a) Processed fairly and lawfully;
(b) Processed for limited purposes and in an appropriate way;
(c) Adequate, relevant and not excessive for the purpose;
(d) Accurate;
(e) Not kept longer than necessary for the purpose;
(f) Processed in line with data subject's rights;

(g) Secure; and
(h) Not transferred to people or organisations situated in countries without adequate protection.

5. Satisfaction of the principles

In order to ensure that the Law Society satisfies the eight data protection principles it will:-

- Ensure that personal information is processed in a fair and lawful manner. This includes ensuring that the data subject has consented to the processing and that the processing is necessary for the legitimate interest of the data controller or the party to whom the data is disclosed.
- When sensitive personal information is being processed, more than one condition must be met and in most cases the Law Society will ensure that the data subject's explicit consent to the processing of such data is obtained;
- Ensure that personal information may only be processed for the specific purposes notified to the data subject when the data was first collected;
- Personal information will only be collected to the extent that it is required for specific purposes notified to the data subject. Any data which is not necessary for that purpose will not be collected in the first instance;
- Personal information must be accurate and kept up to date;
- Ensure that personal information is not kept longer than it is necessary for the purposes used by the Law Society; and
- Ensure that data will be processed in line with the data subject's rights.

6. Data security

6.1 We must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal information and against the accidental loss of or damage to personal information. Data subjects may apply to the courts for compensation if they have suffered damage from such a loss.

6.2 Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal information defined as follows:-

(a) Confidentiality means that only people who are authorised to use the data can access it;
(b) Integrity means that personal information should be accurate and suitable for the purpose for which it is processed;
(c) Availability means that authorised users should be able to access the data if they need it for authorised purposes. Personal information should, therefore, be stored on our centralised computer system.

6.3 Our security procedures include:-

(a) Entry controls – any stranger seen in entry controlled areas should be reported;
(b) Swipe cards are required to access areas where personal information is stored;
(c) Confidential waste disposal;
(d) Equipment – data users should ensure that individuals monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended;

7. Subject access requests

7.1 A formal request from a data subject for information that we hold about them must be made in writing. Any member of staff who receives a written request should forward it immediately to their line manager or the Data Protection Officer.

8. Monitoring and review of this Policy

8.1 This Policy is reviewed on an annual basis by the Chief Executive. Any breach will be taken seriously and may result in formal action.

8.2 We will continue to review the effectiveness of this Policy and to ensure that it is achieving its stated objective.