DATA PROTECTION POLICY

INTRODUCTION

This Policy ("**Policy**") sets out the 9 Data Protection Principles which I, Richard Gareth Griffiths ("**Notary**") commit to comply with when processing personal data in the course of my business as a notary public ("**Business**").]

The Business has notified its data processing activities to the Information Commissioner's Office under registration number: ZI50913X].

The Appendix contains a Glossary of the defined terms in this Policy.

COMPLIANCE WITH THIS POLICY

The Business will ensure the protection of personal data in accordance with this Policy by the Notary, all Personnel and Suppliers.

A breach of data protection laws by the Notary, any Personnel or Supplier could result not only in monetary penalties awarded against the Business but also negative publicity which could affect the Business as well as the entire notaries' profession.

THE DATA PROTECTION PRINCIPLES

The Business shall comply with the following 9 Data Protection Principles when processing personal data.

1. **Fairness and Transparency:** The Business must process personal data fairly and provide individuals with information about how and why their personal data is processed.

The Business must provide a privacy notice to each client, Personnel and Supplier to inform them of:

- the identity of the Business as data controller;
- the purposes for which their personal data are processed;
- the legal basis for processing;
- any legitimate interests pursued by the Business or a third party, if applicable;
- the recipients or categories of recipients of the personal data, if any;
- where applicable, the fact that the Business intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the relevant authority, or reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available;
- the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
- the existence of the right to withdraw consent at any time, if applicable;
- the right to lodge a complaint with a supervisory authority;
- whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data; and
- the existence of Automated Decisions, including profiling, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

For example, such privacy notice should be included in each client engagement letter or service agreement. If no engagement letter is issued, the privacy notice can be made available on the Business website or in other appropriate and easily accessible form. If the notice is published on the website, a conspicuous link to the website or privacy notice should be included in the Business email footer or other Notary stationery to bring the notice to the data subjects' attention.

Where a client provides personal data of third party data subjects to the Business, no notice will have to be provided to those third party data subjects by the Business if such information must remain confidential subject to an obligation of professional secrecy. To the extent that no such obligation of professional secrecy applies, the Business should place a contractual obligation on each client and Supplier to ensure that such notice is provided to those third party data subjects on behalf of the Business.

2. **Lawful Processing:** The Business must only process personal data, including sensitive personal data, lawfully where it has a valid basis for the processing.

Generally, personal data must not be processed without a legal ground. In the context of the Business, personal data are typically processed on the basis of:

- processing is necessary for the performance of a contract (e.g. engagement letter) to which the data subject (e.g. the client) is party or in order to take steps at the request of the data subject prior to entering into a contract;
- processing necessary for the legitimate interests pursued by a client or the Business, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject. This ground may apply to the processing of the personal data of any third party data subjects whose personal data are provided by the client;
- a legal obligation to which the Business is subject and where compliance with such obligation necessitates the processing of personal data by the Business;
- data subject's consent, where such consent is procured from the client; and
- other legal grounds.

3. **Purpose Limitation:** The Business must only collect personal data for a specific, explicit and legitimate purpose. Any subsequent processing should be compatible with that purpose, unless the Business has obtained the individual's consent or the processing is otherwise permitted by law.

The Business will typically process:

- the personal data of its clients as required for the purposes of providing its professional services and the administration of its client relationships;
- the personal data of its Personnel as required for the administration of Personnel, if applicable;
- the personal data of its Suppliers as required for the administration of its Supplier relationships, if applicable; and
- the personal data of its clients, Personnel and Suppliers as is necessary in order to comply with its legal obligations.

The Business will generally not carry out any unsolicited electronic marketing, but to the extent it does, it will have to comply with the law.

4. **Data Minimisation:** The Business must only process personal data that is adequate, relevant and limited to what is necessary for the purpose for which it was collected.

The Business should place a contractual obligation on each client to ensure that only the minimum necessary personal data is provided in connection with the professional services sought.

Where a client provides personal data that appears excessive in connection with the professional services sought, the Business will return such personal data to the client and request that an adequate record of personal data is provided.

5. **Data Accuracy:** The Business must take reasonable steps to ensure personal data is accurate, complete, and kept up-to-date.

The Business should place a contractual obligation on each client to ensure that any personal data provided in connection with the professional services sought is accurate, complete and up to date.

The Business will endeavour to keep an accurate record of personal data in relation to its clients and Personnel.

6. **Individual Rights:** The Business must allow individuals to exercise their rights in relation to their personal data, including their rights of access, erasure, rectification, portability and objection.

The Business will ensure that all Individual Rights Requests are correctly identified and appropriately responded to, subject to any applicable exemptions.

7. **Storage Limitation:** The Business must only keep personal data for as long as it is needed for the purpose for which it was collected or for a further permitted purpose.

The Business will keep all records as long as required by applicable law or as may be necessary having regard to custom, practice or the nature of the documents concerned. For example, the Notaries Practice Rules 2014 require that that notarial acts in the public form shall be preserved permanently. Records of acts not in public form shall be preserved for a minimum period of 12 years.

Save for personal data included in records which must kept for a prescribed period or preserved permanently in compliance with any legal obligations to which the Business is subject, such as the obligation explained above, personal data shall be kept for no longer than necessary for the relevant purpose. For example, any Personnel records should be kept for no longer than 12 months following the termination of employment or contract, unless a longer retention is required under applicable law.

8. **Data Security:** The Business must use appropriate security measures to protect personal data, including where third parties are processing personal data on our behalf.

The Business will adopt the following security measures:

Physical security measures

- ensure physical security of premises, e.g. locked office;
- keep documents in locked cabinets;
- reduce access privileges to only those needed;
- grant access to only such Personnel who need to have access in connection with their duties;
- dispose of documents using a confidential bin or through a cross cut shredder; and
- other appropriate physical security measures.

Organisational security measures

- vet Personnel and Suppliers on a continuing basis;
- implement non-disclosure agreements prior to entering into formalised agreements;
- provide training to Personnel where appropriate;
- implement a strict ban on the use of personal email for work purposes; and
- other appropriate organisational security measures.

Technical security measures

- firewalls which are properly configured and using the latest software;
- regular patch management and OS updates;
- real-time protection anti-virus, anti-malware and anti-spyware software;
- user access control management by, for example, the UAC functionality in Windows, adopting principle of least privileges;
- unique passwords of sufficient complexity and regular (but not too frequent) expiry;
- encryption of all portable devices ensuring appropriate protection of the key;
- data backup; and
- other appropriate technical security measures.

The Business will comply with *Policy: Appointing Suppliers*.

9. **Accountability:** I must take steps to comply with, and be able to demonstrate compliance, with the Data Protection Principles.

The Business will implement appropriate governance processes as set out in this Policy.

GOVERNANCE PROCESSES

In order to ensure that the Data Protection Principles are implemented the Business shall adopt the following governance processes.

A. Documented Policies

In order to ensure compliance with Data Protection Principle 9 (Accountability), the Business shall comply with this Policy and implement such other data protection policies and establish internal governance processes from time to time as may be required in order to operate the Business in compliance with data protection laws.

B. Assurance

The Business will ensure, by way of training or otherwise, that Personnel carry out their tasks in a way that will ensure compliance with data protection laws. Each member of Personnel and each Supplier shall have access to this Policy and it shall have an obligation to comply with it.

Each Supplier will have to comply with data protection obligations in accordance with its service agreement including, where appropriate, a data processing agreement.

The Business shall periodically review this Policy and other policies to ensure that they continue to comply with the relevant legal requirements.

C. Advice

Where necessary the Business shall seek advice in order to ensure that its processes comply with data protection laws.

D. Third Parties

The Business shall comply with *Policy: Appointing Suppliers* in relation to appointing any third party contractor or supplier who will process personal data on behalf of the Business.

E. Data Protection Impact Assessments

The Business shall implement a process so that any processing which is likely to result in a high risk to the rights and freedoms of individuals is subject to a documented Data Protection Impact Assessment (**DPIA**), to assess the risks associated with the proposed processing and identify any

safeguards which should be put in place to mitigate those risks. The Business shall maintain a record of each DPIA.

F. Record-keeping

The Business will implement a process to maintain an up-to-date documented record of its processing activities by way of adding relevant information in the Notary register or by other appropriate means. This record should include a general description of the following:

Record keeping requirements	Suggested record
• The purpose of the processing.	• Typically, in relation to Business transactions this will include processing to deliver client services;
• The categories of personal data and individuals to whom the data relates.	• a variety of mostly legal documents with copies of identity information relating to clients;
• The categories of recipients (if any), including both data controllers and data processors, and any transfers outside the European Economic Area (EEA).	• either the client or a third party to whom the client wished the documents to be sent after processing and such parties may often be located outside the EEA;
• Where possible, the envisaged retention period for the personal data.	• records will be retained in accordance with the Notaries Practice Rules; and
• Where possible, a general description of the technical and organisational security measures in place.	• the measures in place as set out at paragraph 8 above.

Although it is envisaged that the Business will act as data controller in the majority of cases, where the Business processes personal data on behalf of another person the Business will make sure to maintain a record of its activities as a data processor and/or data controller. This record should include a general description of the following:

- The identity of the Business and contact details.
- The categories of processing carried out on behalf of the third party.
- Any transfers outside the EEA.
- Where possible, a general description of the technical and organisational security measures in place.

G. Privacy By Design

When implementing a new processing activity, tool or functionality involved in the processing of personal data, the Business will ensure, by contractual means or otherwise, that such activity, tool or functionality is designed and built in a way that allows me to comply with the Data Protection Principles.

H. Complaint handling

The Business shall implement a process to receive and handle enquiries and complaints from individuals and the supervisory authorities concerning the processing of personal data.

The Business shall ensure that all enquiries and complaints are dealt with in a timely manner, in compliance with any applicable statutory deadlines.

Last updated August 2017

APPENDIX: GLOSSARY

anonymous data	Data which does not relate to an identified or identifiable individual, or personal data which has been rendered permanently anonymous in such a way that the individual is no longer identifiable (even if the data was combined with other data held by the Business Company).
Automated Decision	A decision which produces legal effects, or similarly significantly affects an individual, and which is based solely on the automated processing (including profiling) of their personal data.
Business	The business of providing notarial services.
controller	A party which determines the purposes and means of the data processing.
data	Any information which is recorded electronically or, where recorded in a manual format (e.g. on paper), is organised by reference to an individual.
data subject	The individual to whom the personal data relates.
Individual Rights Request	A request from a data subject in respect of their personal data, e.g. to access, erase, or rectify their personal data, or object to its processing.
personal data	Any data relating to an identified or identifiable natural person. This can include (but is not limited to) names, addresses, email addresses, positions held, photographs, job applications, personnel files, occupational health records, opinions, and correspondence to and from an individual.
Personnel	All employees of the Business at all levels, including, directors, officers, agency workers, seconded workers, volunteers, interns, agents, contractors and external consultants.
processing	Any operation performed on personal data, such as collection, recording, storage, retrieval, use, combining it with other data, transmission, disclosure or deletion.
processor	A party processing personal data on behalf of a controller, under the controller's instructions.
pseudonymised data	Personal data which can only be attributed to a specific individual by combining it with additional information (such as a key or other identifier), where the additional information is kept technically and logically separate from the pseudonmyised data to avoid the individual being identified. Pseudonymised data remains personal data.
Sensitive or special categories personal data	Personal data revealing a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; biometric (e.g. fingerprints or facial recognition) or genetic information; or information about a person's health, sex life or sexual orientation, or relating to criminal convictions or offences (including allegations).
Supplier	Any external vendor, supplier, consultant or similar third party engaged to provide services to the Business.