Leech & Co - Data Protection Policy

Policy information	
Organisation	Leech & Co Solicitors Limited
Scope of policy	This policy applies to all Leech & Co employees: 1. Matthew Connery 2. Claire Taylor All data is stored on a secure remote server controlled and supervised by Emerald Group. The Data Protection Policy of Emerald Group can be found here: http://www.emerald-group.co.uk/_userfiles/pages/files/Emerald_Data_Protection_Policy_Master.pdf The GDPR Technology Plan of Emerald Group is also held by Leech & Co and is available on request. The data processors acting on behalf of Leech & Co include various medical agencies instructed for the purposes of obtaining medical reports in support of client matters. The Data Protection Policies of all medical agencies instructed by Leech & Co are held by Leech & Co and are available on request in writing. This policy also covers the following data processors acting on our behalf: Booth Ainsworth (Accountants) and Eclipse (Proclaim).
Policy operational date	This Data Protection Policy is operational from 25th May 2018
Policy prepared by	The Data Protection Officer for Leech & Co is Matthew Connery (matthewc@leech.co.uk / 0161 749 9000). This policy has been prepared by Matthew Connery.
Date approved by Board	N/A
Policy review date	This policy will be reviewed by 25th May 2021 and/or following a data breach, whichever is the sooner.

Introduction	
Purpose of policy	The purpose of this Data Protection Policy is to: • comply with the law; • follow good practice; • protect clients, staff and other individuals; • protect the organization.
Types of data	Leech & Co controls and processes both personal and sensitive client data i.e. personal data, medical records, medical reports, employment records, financial information and documents etc. Leech & Co will either obtain the data directly from the data holder i.e. medical treatment provider, employer etc or use an agency i.e. a medical agency. The data is held and processed with the client's consent and for the performance of the contract between Leech & Co and the client. Leech & Co also hold employee data e.g. contracts, sick notes etc, which is held for the employee's legitimate interests.
Policy statement	Leech & Co hereby commit to: • comply with both the law and good practice; • respect individuals' rights; • be open and honest with individuals whose data is held; • provide training and support for staff who handle personal data, so that they can act confidently and consistently; • Notify the Information Commissioner voluntarily, even if this is not required. Leech & Co further commit to report *serious* breaches of data protection to the ICO in circumstances where the following occur: 1. There is detriment to the data subject i.e. potential exposure to identity theft, private information being disclosed etc; 2. The volume and/or sensitivity of the data lost / released / corrupted is considered serious; N.B. If there is uncertainty as to whether the breach constitutes a serious breach, Leech & Co will presume the breach is serious and will report it accordingly.

	Leech & Co commit to uphold individuals' right with regard to data protection as defined in the GDPR, as follows: • 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 • Rights in relation to automated decision making and profiling.
Key risks	Leech & Co have two main risk areas in terms of data breaches: • Data getting into the wrong hands i.e. due to a security breach or inappropriate disclosure of information; • Data being disclosed in error and/or without consent; • Data being inaccurate and/or out of date.

Responsibilities	
Company Director	Matthew Connery, the Director of Leech & Co, has overall responsibility for ensuring that Leech & Co complies with its legal obligations under the GDPR.
Data Protection Officer	Matthew Connery is the Data Protection Officer (DPO) for Leech & Co. His responsibilities include: • Reviewing Data Protection and related policies • Advising other staff on tricky Data Protection issues • Ensuring that Data Protection induction and training takes place • Notification to the ICO • Handling subject access requests • Approving unusual or controversial disclosures of personal data • Approving contracts with Data Processors
Specific Department Heads	During the initial Operational Period (see above), there are no department heads to assume responsibility for specific data protection issues within departments. Matthew Connery will retain overall responsibility for all data protection issues.
Employees & Volunteers	All staff will be required to read, understand and accept the policies and procedures that relate to the personal data they will handle in the course of their work. This will apply to all new employees as part of the induction training.
Enforcement	A full internal inquiry led by Matthew Connery will follow a data breach (either serious or not serious) and/or non-compliance with the Data Protection Policy. A report will be compiled following interview of the staff member which will be kept within the GDPR file. On the basis of the outcome of the inquiry, the sanctions may include disciplinary procedure and/or re-training. All staff will be aware through training that all breaches (either serious or not serious) will be reported immediately to Matthew Connery.

Security	
Scope	The Data Protection Policy applies to all data controlled or processed by Leech & Co in the course of business. See also the Leech & Co Business Continuity / Disaster Planning policy.
Setting security levels	The data controlled or processed by Leech & Co may contain sensitive and personal information, for example medical records, employment records, financial records etc and consequently all data will be accorded the highest security level.
Security measures	Leech & Co security measures include: 1. All clients must authorise disclosure of data i.e. medical records, medical reports, information specific to the case, personal information etc in writing; 2. Staff members will not disclose personal and/or sensitive data over the telephone and will only do so when in receipt of a written request and the client's written authority; 3. All data is stored electronically and not on paper (Leech & Co are a paperless firm); 4. All access to the Case Management system is password protected and specific to the staff member; 5. The data is stored on a remote server, subject to regular backup, and access to it is password protected.
Business continuity	All data controlled or processed by Leech & Co is stored on a remote server which is regularly subject to backup and is password protected. See Data Protection Policy of Emerald Group. Claire Taylor will become the Data Protection Officer for Leech & Co in the event of the absence of Matthew Connery. See also Leech & Co policy for Business Continuity / Disaster Planning.
Specific risks	Leech & Co have identified specific circumstances which give rise to a potential breach of data and have formulated precautions, as follows: 1. Telephone requests for information – all staff members are trained not to disclose or receive personal and/or sensitive data over the telephone. This includes contact details,

	information specific to the client's case etc. This is to avoid vishing or phishing methods. All personal and/or sensitive data is only to be disclosed or received in writing and with the written consent of the client; 2. All personal and/or sensitive data received on a mobile telephone i.e. via text, Whatsapp, Facebook etc, will be transferred immediately to the secure Case Management System and the original data removed from the mobile device; 3. All personal and/or sensitive data provided to Leech & Co in a meeting with the client, at the client's home etc, will be recorded and stored on the Case Management System and not in an unsupported document i.e. in Word, Excel etc.

Data recording and storage	
Accuracy	Leech & Co will ensure the accuracy of any data provided by the client or by a third party over the telephone, by text, social media or by e-mail by providing written confirmation of the data provided to the client i.e. by letter or by e-mail, and requesting the client to confirm the accuracy of the data provided.
Updating	The data processed by Leech & Co may require updating during the course of a client matter, for example it may be necessary to obtain updated medical records. Each data request will follow the same procedure as above i.e. the client is notified of the need to update the data and the client will provide consent in writing.
Storage	All data provided by clients or by third parties will stored on the Case Management System which is supported only on the remote server controlled and supervised by Emerald IT Management.
Retention periods	Digital copies of all data relating to a case will be stored on the Case Management System for the period as required by professional regulations i.e. 6 years, from the date of the conclusion of the case. The data will then be digitally archived. In the case of copy documents, paper copies of data provided by the client and/or by third parties will be destroyed at the time the data is transferred to the Case Management System. In the case of original documents, these will be returned to the client and/or the third party at the time the data is transferred to the Case Management System.
Archiving	Digitally stored data will be archived at the expiry of the period as required by professional regulations i.e. 6 years from the date of the conclusion of the case. See above in relation to paper copies of documents. Leech & Co will not hold and therefore will not archive paper copies of documents at the conclusion of the case.

Right of Access	
Responsibility	Matthew Connery has responsibility for all data access requests. Matthew Connery will log the request upon receipt and it will be dealt with within one month of receipt. All employees have a responsibility for passing on all data access request, or what may be construed as data access requests, to Matthew Connery upon receipt.
Procedure for making request	It is Leech & Co policy that all data access requests must be in writing and must be accompanied by photo identification. Data access requests will not be accepted over the telephone, by text or by social media. The data access request will be dealt with within one month of receipt.
Provision for verifying identity	The identity of the person making the data access request will be verified by Matthew Connery using the identification document(s)/report on file and by a written response to the written request.
Charging	Leech & Co will provide the requested data free of charge except in certain circumstances when a reasonable fee will be charged i.e. excessive and/or repeated demands, requests for further copies of data already provided etc. The circumstances in which the fee will be charged will be defined by Leech & Co and confirmed to the client upon receipt of the request. The reasonable fee will be based on the administrative cost of providing the data and will be confirmed to the client upon receipt of the request and should circumstances exist to warrant the charging of the said fee. Should the client not agree to the application of the fee or the fee itself, the matter will be referred by either Leech & Co or the client to the ICO for further guidance.
Procedure for granting access	The requested data will be provided to the client in a commonly used electronic format of the client's choice. If the client does not wish to receive the data in an electronic format, the data will be provided on paper and provided to the client by trackable post. All data is stored on the secure Case Management System and is available to be provided to clients upon request.

Transparency	
Commitment	Leech & Co will ensure that all clients are provided with written confirmation as to the following: • The purpose the data is required; • What type of disclosure of the data is likely; • The parties the data will be disclosed to. This Data Protection Policy will be available to all clients on the Leech & Co website. All clients will be made aware of the location of the policy and it will be made available to them on request.
Procedure	The Data Protection Policy will be available to all clients on the Leech & Co website. All clients will be informed of the Data Protection Policy, and it's location on the website, in the initial client care letter.
Responsibility	All clients will be informed in the initial client care letter that Matthew Connery is responsible for all data access requests and data issues. The client care letter will also confirm that any such requests or issues should initially be provided to the file handler to be passed to Matthew Connery.

Lawful Basis	
Underlying principles	Each client will provide Leech & Co with written consent to process personal and sensitive data and this data will only be processed with such consent. The processing of personal and sensitive data is necessary to allow Leech & Co to carry out the terms of the contract between Leech & Co and the client. Leech & Co cannot carry out the terms of the said contract without processing this data. If a client will not consent for Leech & Co to process his/her data in a way that is necessary to carry out the terms of the said contract, then Leech & Co will advise in writing that the terms of the contract cannot be carried and the contract may be terminated.
Opting out	The client is entitled to withhold his/her consent or opt out of providing consent for Leech & Co to process his/her data in particular ways. If this withdrawal or consent or opting out of providing consent means that Leech & Co cannot act for this client, then the client will be advised in writing accordingly.
Withdrawing consent	The client may withdraw consent for Leech & Co to process data, but this withdrawal of consent cannot be retrospective. Leech & Co are legally obliged to hold data for a client for 6 years after the conclusion of the case. This obligation overrides the withdrawal of the client's consent to process his/her data.

Employee training & Acceptance of responsibilities	
Induction	All Leech & Co employees will be informed of their responsibilities with regard to all types of personal data during their induction procedure. As part of the induction procedure, all Leech & Co employees will be required to read the Data Protection Policy.
Continuing training	All Leech & Co employees will receive ongoing training either via outside sources or internal training sessions / meetings. As part of this ongoing training, Data Protection issues will be raised where appropriate and necessary.
Procedure for staff signifying acceptance of policy	All Leech & Co employees will be required to read the Data Protection Policy and will receive ongoing training with regard to it. All employees will be required to confirm in writing that they have read and understood the terms of the Data Protection Policy and their responsibilities with regard to it.

Policy review	
Responsibility	Matthew Connery will be responsible for the next policy review.
Procedure	As part of the policy review, all employees will be consulted to ensure the policy is working and complied with and whether any amendments will be required.
Timing	The review will commence 6 months prior to the review date to ensure any changes and required training will be complete by the review date. Therefore, the review will commence on 25th November 2020.