Data Protection Policy

1 Introduction

1.1 The General Data Protection Regulation (Regulation (EU) 2016/679, is a regulation in EU law on data protection and privacy for all individuals within the European Union. The aim of the regulation is primarily to give control to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. It also addresses the export of personal data outside the EU. The regulation has now been adopted by the UK as the General Data Protection Regulations 2018 (GDPR), effective from 25th May 2018. [The GDPR and associated legislation The Data Protection Act 2018 replace the Data Protection Act 1998, which originally came into force on the 1st March 2000 and is now repealed].

1.2 The directors and management team at Yarwood Holmes Law Limited are fully committed to compliance with the requirements of the GDPR and associated data protection legislation. The firm will therefore follow procedures that aim to ensure that all directors, consultants, employees, contractors, suppliers, agents and anyone directly associated with the firm or who have access to any personal data held by or on behalf of the firm, are fully aware of and abide by their duties and responsibilities under the regulations.

> Warning: Failure to comply with the firm's policies, as set out in this manual, may be treated as gross misconduct and result in disciplinary action.

2 Summary

2.1 All businesses use personal data gathered from customers or clients, suppliers and work colleagues in some way or another. It is in our collective interest to protect this data and keep it confidential in line with existing regulations and common sense.

2.2 Data protection regulations determine how our business controls and processes personal information, including how we may collect it, the situations in which we are permitted to use it, and for how long we may retain it. Effective from 25 May 2018, the General Data Protection Regulation (GDPR) replaces the national data protection laws in all EU member states. The GDPR enhances the rights of individuals by furthering the rights associated with individuals' personal data held in certain locations. It also covers the portability of data sets from one organisation to another. In addition, the GDPR encourages businesses to set up processes and procedures in a way that does not involve collection or retention of more personal data than is needed. Penalties for non-compliance can be severe including significant fines and reputational damage.

2.3 The GDPR covers the critical area of obtaining, using, storing, managing and deleting personal data, and represents a substantial regulatory expansion of personal data protection rules and requirements.

3 Policy statement

3.1 In order to operate efficiently, the firm has to collect and use information about people with whom it works. This will include for example current, past and prospective employees, clients and suppliers. In addition, it may be required by law to collect and use information in order to comply with the requirements of government legislation (e.g. Money Laundering Regulations 2017) or in accordance with service delivery contracts (e.g. Legal Aid Agency). This personal information must be protected and dealt with properly, irrespective of how it is collected or stored, whether it be in hard copy, computer records, DVD, CCTV or simply an IP address from a website enquirer.

3.2 Personal information is anything that allows a living person to be identified either directly or indirectly, and can include a name, address, email address, financial details, phone number and even job title. The GDPR refers to sensitive data as "special categories" of personal data including details of trade union membership, political preferences, racial or ethnic origin, sexual orientation, religious or other beliefs of a similar nature and physical or mental health conditions.

3.3 We should remind ourselves that everyone has a responsibility for maintaining confidentiality in relation to all client matters and data. Staff must ensure that any and all personal data that comes into their possession is protected in whatever format it is received (paper, electronic etc). This particularly applies to information that can be stored on electronic devices such as USB/flash or pen drives, computers, mobile phones etc. If this information leaves the premises in any format, either on paper or electronically, then the individual concerned must be responsible for ensuring that documents are safely and securely stored (i.e. not left in cars), that electronic devices are encrypted and/or password protected, and that discretion is applied when opening such information in public spaces.

3.4 The firm regards the lawful and correct treatment of personal information as very important to its successful operations and to maintaining confidence between the firm and those with whom it carries out business. The firm will ensure that it treats personal information lawfully and correctly.

3.5 To assist in establishing what level of security is right for our business we will review annually the personal data we hold and assess the risks to that information as part of our annual quality review.

3.6 In addition, as part of a data protection by design approach, we will conduct a data protection impact assessment (DPIA) in specific circumstances to assess privacy risks. We will undertake a DPIA before we begin any type of processing which is "likely to result in a high risk". This means that although we may not yet have assessed the actual level of risk, we will screen for factors that point to the potential for a widespread or serious impact on individuals. We will conduct a DPIA at any stage where changes to our operating system or procedures are proposed or where planned changes or upgrades are planned in relation to hardware or technology. We will consider all processes involved in the collection, storage, use, sharing and disposal of personal data. We will consider how sensitive or confidential the data is and what damage or distress could be caused to individuals, as well as the reputational damage to our business, if a security breach occurred. See below for further information about the procedure to be adopted when conducting a DPIA.

3.7 Having conducted the DPIA we will then begin to choose the security measures that are appropriate for our needs.

3.8 Regular DPIAs supports the GDPR's accountability principle, helping organisations demonstrate compliance. Conducting a DPIA can also help increase awareness of privacy and data protection issues within an organisation.

4 Data Protection

4.1 We will be registered as a Data Controller with the Information Commissioner (ICO). The types of personal data that we process will be listed under our registration records. All information that we hold concerning individuals will be held and processed lawfully in accordance with the provisions of the Data Protection Regulations.

4.2 We have appointed a Data Protection Officer (DPO) who is Helen Holmes (HH), and she is assisted in this role by the practice manager Helen Liffen (HL).

4.3 The Data Protection legislation requires every data controller who is processing personal data, to notify the ICO and renew their notification on an annual basis. Failure to do so is a criminal offence. It is the responsibility of the DPO to ensure that registration remains up to date. Any changes to the register must be notified to the Information Commissioner within 28 days.

4.4 We keep information passed to us confidential and respect rights to privacy. We will keep personal information confidential except to the extent that it is necessary to disclose it by law or to comply with a regulatory or legal process or where we need to process the information to provide a contract, product or service. We therefore rely on the following bases for the lawful processing of data as set out in Article 6 of the regulations:

- Contract: the processing is necessary for a contract we have with the individual, or because they have asked us to take specific steps before entering into a contract and
- Legal obligation: the processing is necessary for us to comply with the law (not including contractual obligations)

4.5 We have procedures designed to ensure that personal data is used only by appropriately authorised and trained personnel, and to safeguard such information against accidental loss or unauthorised disclosure.

4.6 Those individuals about whom we process data have a right, under the Data Protection Regulations, to obtain the personal data that we hold on them. Therefore, if any member of staff receives a request designated as a Data Subject Access Request (DSAR) or enquiry from any individual concerning this right, you MUST notify our Data Protection Officer immediately as strict time limits apply in dealing with such requests. We must comply with access rights without delay and within a month in any event. All DSAR will be logged and recorded by the DPO for monitoring purposes on the firm's Data Map.

4.7 Providing access to personal data that we hold about an individual is free of charge although we may charge or refuse a request if it is deemed to be manifestly unfounded or excessive. A decision to refuse a request can only be made by the DPO or in his absence the COLP or another director in the firm, and if we refuse a request, we must explain why and how any complaint about our decision may be made.

4.8 Further guidance about dealing with Data Subject Access Requests is available on the ICO website. www.ico.org.uk

4.9 We must also observe the principles that underpin the Regulations as stated in Article 5, namely that all data covered by the Act (which includes not only computer data, but also personal data held within a filing system) is:

a) "processed lawfully, fairly and in a transparent manner in relation to individuals.

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for

archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

g) not transferred to another country without appropriate safeguards being in place, and:

h) made available to Data Subjects and allow Data Subjects to exercise certain rights in relation to their Personal data.

4.10 It is the responsibility of the Data Protection Officer to ensure that all personnel, including senior management, are aware of their obligations under Data Protection Regulations and associated legislation and are provided with any appropriate updates as to how they are required to support the practice in ensuring compliance.

5 Data subject access requests and other rights

5.1 Data protection legislation provides the following rights to the individuals for whom we process personal data:

a) the right to be informed – Individuals have the right to receive “privacy information” and be informed about the collection and use of their personal data, including the purposes for our processing of their personal data, our retention periods for that personal data, and who it will be shared with.

b) the right of access – individuals have the right to access their personal data and supplementary information including confirmation that their data is being processed by us, access to their personal data; and other supplementary information largely corresponding to the information provided in our privacy notice. Access must be provided free of charge (unless a request is manifestly unfounded or excessive, particularly if it is repetitive). Information (in most circumstances) must be provided without delay and at the latest within one month of receipt. For this reason, any individual requesting to apply their access rights under the regulations must report

the request immediately to our Data Protection Officer. Further information about the effective processing of access requests can be found on the ICO website.

c) the right to rectification – the regulations give the right to individuals to have personal data held about them to be rectified if it is inaccurate or incomplete. A request for rectification must be implemented within one month. For this reason, any individual requesting to apply their rectification rights under the regulations must report the request immediately to our Data Protection Officer. Where we decide not take action in response to a request for rectification, we must explain why to the individual, informing them of their right to complain to the ICO and/or to seek a judicial remedy.

d) the right to erasure – the broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no proper reason for its continued processing. The right to erasure does not provide an absolute 'right to be forgotten' for the individual and there may be circumstances when other legal authorities will apply. Any requests under this right must be reported immediately to the Data Protection Officer for consideration.

e) the right to restrict processing – the regulations allow an individual to suppress the processing of personal data. When processing is restricted, we are permitted to store the personal data, but not further process it.

f) the right to data portability – this right allows individuals to obtain and reuse their personal data for their own purposes across different services. This right is extremely unlikely to be applied currently in legal services but allows individuals to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability. This right is intended to enable consumers to take advantage of applications and services which can use this data to find them a better deal or help them understand their spending habits.

g) the right to object – individuals have the right to object to processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling); direct marketing (including profiling); and processing for purposes of scientific/historical research and statistics. It is likely that individuals about whom we process personal data may exercise the right to object only under direct marketing and we must stop immediately if such a request is received. Our direct marketing will have a right to object notice on it with details of how to contact us to make an objection.

h) rights in relation to automated decision making and profiling – the regulations have provisions on individuals' rights in relation to automated individual decision-making (which making a decision solely by automated means without any human involvement)and profiling (automated processing of personal data to evaluate certain things about an individual). Neither of these types of processing is used in our delivery of services.

5.2 All Data Subject Access Requests (DSAR) must be referred to the DPO at the earliest opportunity to ensure the deadline for response is met. This can be done simply by passing the item of correspondence via internal mail (retain a copy until you have confirmation of receipt then destroy), scanned copy via email or simply by confirming the request via the phone. Copies of requests should also be passed to HL for recording on the firm's Data Map and for monitoring purposes to ensure timescales and deadlines are met.

5.3 Although the DPO has overall responsibility for ensuring records of DSAR's are appropriately maintained it is the responsibility of LS to ensure the Data Map records the date of receipt of the DSAR along with the date of response and outcome or decision. The DPO will retain a

file or record, either in paper form or an electronic copy, of the request together with the firm's response including a summary of the Data provided, where appropriate. This information will be stored on the firm's server and be retained for a period of no more than 6 years after which time the records will be deleted. Hard copies of documents received or produced will be destroyed immediately upon scanning or saving to the electronic file.

6 Data breaches

6.1 The data protection regulations enforce a duty on our firm to report certain types of personal data breaches to the ICO. We will usually have a maximum of 72 hours, after becoming aware of the breach, to report the circumstances to the ICO. All staff must ensure that any suspected breach is reported to the Data Protection Officer immediately.

6.2 A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data. The breach may be accidental or deliberate. Examples provided on the ICO's website include:

- Access by an unauthorised third party.
- Deliberate or accidental action (or inaction) by a controller or processor.
- Sending personal data to an incorrect recipient.
- Computing devices containing personal data being lost or stolen.
- Alteration of personal data without permission and.
- Loss of availability of personal data through for example encryption by ransomware or accidental loss or destruction.

6.3 This is not a comprehensive list so all concerns relating to personal data breaches must be referred to the Data Protection Officer.

6.4 The Data Protection Officer will decide whether the breach is reportable to the ICO and if there is a high risk of detrimental impact on an individual's rights, the DPO will report the incident to the individual affected and provide advice and assistance about how the individual may protect themselves from the impact of a personal data breach. There may be occasions when it is also necessary to report such a breach to the Solicitors Regulation Authority (SRA). This decision will be made by the DPO who is also the COLP.

6.5 The breach report, if made to the ICO, will contain a description of the data breach including:

- Reference to the categories and number of individuals affected.
- The categories and number of personal data records affected.
- The name and contact details of our Data Protection Officer
- An assessment of the likely impact of the personal data breach and the likelihood of the impact occurring.
- A description of the measures taken or proposed to be taken to deal with the breach and to prevent it from occurring again in the future.

6.6 A record of all personal data breaches will be maintained by the DPO/practice manager on the Data Map (see below) and these will be separated as between reported and non-reported incidents. All breaches will be reported to the directors of the firm as part of the COLP monthly report. When considering whether a breach is reportable, the Data Protection Officer will refer to the ICO's guidance that can be found at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

6.7 Any member of staff who becomes aware of a possible data breach must notify the DPO and HL immediately and upon receipt of this information. HL will arrange to record, on the firms Data Map spreadsheet, the date of occurrence and action taken to remedy the breach together with the date of response, including whether the matter was reportable to the ICO and/or the data subject. The DPO will retain a record of all correspondence etc associated with the breach, either in paper form or an electronic copy. This information will be stored on the firm's server and be retained for a period of no more than 6 years after which time the records will be deleted. Hard copies of documents received or produced will be destroyed immediately upon scanning or saving to the electronic file.

7 Privacy Policy

7.1 The firm's privacy policy on our website reflects the requirements of GDPR and confirms the basis for collecting data, details the type of data we collect, describes how we use it, provides a summary of data subject rights and explains how we satisfy the new regulations. We aim to ensure that we draw to the attention of all existing and new clients our privacy policy either via the website or within our terms of business.

7.2 Use of client information outside the European Union: In order to provide the client with requested products and services we may need to transfer personal information to service partners based in countries outside the European Economic Area (EEA). Our Terms of Business confirms to the client that this will not affect their rights and the firm will take all reasonable steps necessary to ensure that any personal information transferred outside the EEA will be treated securely and in accordance with our Privacy Policy.

8 Disclosure of personal information and consent/refusal

.

8.1 We may disclose personal information to any of our employees, officers, insurers, professional advisers, consultants, agents, suppliers or subcontractors insofar as reasonably necessary for the purposes set out in our policy and in the delivery of our services.

8.2 Where we may be required to disclose information within a file for the following reasons, we will seek prior consent of the data subject at the earliest opportunity:

- To progress your case i.e. to discuss your file with Experts, Counsel, Costs Specialists etc or
- To assess the firm's compliance with its regulatory obligations and to obtain or maintain specialist quality accreditations [by e.g. Law Society approved consultants/ assessors and/or our external compliance advisors]

8.3 We will always obtain a Confidentiality Undertaking from third parties before we share any information with them.

8.4 In any case where a client refuses consent to disclosure either at the outset of the case or during the period the personal information on the data subject is being held (and where the 3rd party disclosure is not directly associated with the delivery of our legally contracted services) we will mark the file accordingly and record on the notes section of the client record (where available) on our case management system to show; "consent refused". Under no circumstances is the content of the file or electronic record to be disclosed to a 3rd party without reference to and the authority of the DPO. In appropriate circumstances express consent of the data subject will be requested again.

9 Retaining personal information

9.1 Personal information that we process for any purpose shall not be kept for longer than is necessary. Within our Data Map we have documented the timescales for retention of Personal Data, and these will be subject to review annually as part of our AQR.

9.2 Without prejudice to other obligations set out in this policy or our legal obligations, we will usually delete personal data falling within the categories set out below at the date/time set out below:

a) personal and sensitive data including marital status, religion, race, gender, sexual orientation, dependants, dependants' names, medical history, criminal history, property related details, financial status – debt, CCJ, nationality, employment status, employer details where relevant, to which you explicitly consent.

b) when you ask us to erase your data compliant with GDPR Article 17.

9.3 Notwithstanding the other provisions of this policy, we will retain documents and records containing personal data:

a) to the extent that we are required to do so by law.

b) if we believe that the documents may be relevant to any ongoing or prospective legal proceedings; and

c) in order to establish, exercise or defend our legal rights (including providing information to others for the purposes of fraud prevention and reducing credit risk).

9.4 Where there is no statutory period defined in legislation, our retention period will be based on the period determined in accordance with Law Society guidance and relevant legislation.

10 Privacy by Design and Data Protection Impact Assessment (DPIA)

10.1 Under the GDPR we are required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures, for example Pseudonymisation (see Interpretation below) This must be done in an effective manner to ensure compliance with data privacy principles.

10.2 We will assess what Privacy by Design measures can be implemented on all programmes, system or processes that Process Personal Data by taking into account the following:

- the state of the art.
- the cost of implementation.
- the nature, scope, context and purposes of Processing; and
- the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the Processing.

10.3 Data controllers must also conduct DPIAs in respect to high-risk Processing or when implementing major system or business change programs involving the Processing of Personal Data including:

- use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes) – (e.g. introduction of a new computer-based case management system).
- automated Processing including profiling and ADM.
- large-scale Processing of Special Categories of Personal Data or Criminal Convictions Data; and
- large-scale, systematic monitoring of a publicly accessible area (e.g. introduction of CCTV).

11 When should you conduct a DPIA?

11.1 You require a DPIA when data processing is likely to result in a "high risk" to data subjects. The GDPR says you must conduct a DPIA if you plan to:

- Use systematic and extensive profiling with significant effects.
- Process special category or criminal offence data on a large scale; or
- Systematically monitor publicly accessible places on a large scale.

11.2 The ICO, as required by the GDPR, has also published a list of the types of processing that require a DPIA.

11.3 The European Data Protection Board (EDPB) has endorsed the guidance on DPIAs issued by its predecessor body [the Article 29 Working Party (WP29)]: DPIAs and determining whether processing is "likely to result in a high risk". This identifies nine criteria that might indicate high risk and suggests that, 'as a rule of thumb', processing operations that meet two or more will require a DPIA. The EDPB endorsed guidance also explores the meaning of 'large scale'. This term is not defined in the GDPR beyond the observation in Recital 91 that 'the processing of personal data should not be considered to be on a large scale if the processing concerns personal data from patients or clients by an individual physician, other health care professional or lawyer. In determining what does constitute 'large scale', the WP29 guidance suggests having regard to:

- the number of data subjects concerned, either absolutely or proportionately to the relevant population
- the volume of data and/or range of different data items to be processed.
- the duration or permanence of the data processing activity; and,
- the proposed activity's geographic extent.

11.4 A DPIA is not legally required:

- where a processing is not 'likely to result in a high risk to the rights and freedoms of natural persons'
- in relation to a processing, which is by its nature, scope, context and purpose is very similar to the processing for which a DPIA has been carried out
- where a particular processing is exempt under EU or UK law from a DPIA

11.5 Also processing operations, which existed before 25th May 2018 do not require a DPIA, as the requirements apply to processing operations initiated after the GDPR came into force. However, where significant changes take place to such pre-existing processing, e.g. because of using a new technology or using personal data for new purposes, such changes might be regarded as a new data processing operation and could require a DPIA.

12 What does a DPIA include?

12.1 Article 35(7) identifies four features that DPIAs must contain for them to be sufficiently comprehensive. These are:

- describe the nature, scope, context and purposes of the processing
- assess necessity, proportionality and compliance measures
- identify and assess risks to individuals
- identify any additional measures to mitigate those risks

13 Key elements of a successful DPIA

13.1 A good DPIA helps you demonstrate that you have considered the risks related to your intended processing and met your broader compliance obligations.

13.2 The GDPR does not specify a DPIA process to follow. Instead, it allows organisations to use a framework that complements their existing processes.

14 What steps will we adopt in undertaking a DPIA?

14.1 Any decision on when a DPIA is required will be determined by the DPO and COLP, Helen Holmes. Before doing so she will consult the ICO's guidance on DPIAs. The ICO identifies six steps in the process, and recommends that organisations consult with their internal and external stakeholders as part of the process, which we will do as required.

14.2 We will fully document and integrate the DPIA process into any existing project and risk management procedures as the most effective way of ensuring that all relevant firm issues are covered. This may involve guidance and assistance from 3rd party advisers/processors.

14.3 We will adopt the ICO guidance and even where a mandatory DPIA is not required we may decide, as a matter of good practice, to carry one out. Where we determine that a DPIA is not required we will document our reasoning and basis for this decision.

14.4 In the early stages of any IT transformation project we will consider whether or not a DPIA might be required, we will document this, and review our conclusions as the project develops.

14.5 Our DPO will be responsible for monitoring the performance of the DPIA. Where the processing is being performed, either in whole or in part, by a 3rd party or data processer working on our behalf, we will require the processer to assist the COLP in carrying out the DPIA, including, for example, by providing necessary information, although acknowledging that the firm and DPO/COLP remain ultimately responsible and accountable for the DPIA.

14.6 We will include appropriate provisions in our data processing agreements to ensure that we have all necessary assistance and cooperation from our data processers in relation to any DPIAs we need or wish to undertake.

14.7 We may, in carrying out a DPIA, seek the views of data subjects or their representatives (Article 35 (9)). Depending on the issues arising from the envisaged processing operation, we may also seek advice from independent experts and engage with and seek input from other relevant stakeholders.

14.8 In the unlikely event that we determine that an identified risk to the rights and freedoms of any of our data subjects cannot be sufficiently addressed we will consult the ICO, and provide a copy of your DPIA.

14.9 Any DPIA we produce will be published and available for review at our registered office either in full or in summary form.

14.10 Any DPIA will be subject to ongoing monitoring and review by the DPO/COLP to ensure that new risks are proactively identified and addressed, and that new circumstances are taken into account to ensure on-going compliance. The Article 29 Working Party recommends all DPIAs are monitored on an on-going basis and re-assessed at least every three years.

14.11 The DPIA process is outlined in checklist 10 of the Law Society 'Preparing for the General Data Protection Regulation: A guide for law firms' and you can find the ICO's extensive DPIA guide, awareness checklist and template online.

15 Guidance and training

15.1 All members of staff will receive training and guidance on data protection and confidentiality as part of their induction when joining the firm and when policy or regulatory changes occur. For the purposes of the GDPR a briefing note was issued in May 2018 to all staff and the updated Data Protection policy has been circulated and acknowledged by all staff as having been read. In addition, and each year, the DPO will organise refresher training and/or an update covering key issues and emerging risks to ensure that all staff remain alert and aware of their obligations under the GDPR.

15.2 All directors, staff, consultants, contractors, or any other agents of the firm have been advised that they must:

- ensure that they, and any of their staff who have access to personal data held or processed for or on behalf of the firm, are aware of this policy and are fully trained in and are aware of their duties and responsibilities under the GDPR. Any breach of GDPR will be deemed as being a breach of any contract which exists between the firm and that individual, company or organisation
- Consultants, contractors, or any other 3rd party agents of the firm will be advised that must be prepared to allow verification audits to be conducted to assess compliance (if requested)

15.3 3rd party organisations will be required to indemnify the firm against any prosecutions, claims, proceedings, actions or payments of compensation or damages, without limitation, brought about or arising under GDPR or associated legislation.

15.4 All contractors who process personal information supplied by the firm will be required to confirm that they will abide by the requirements of the GDPR and provide the firm with a confidentiality agreement.

16 Review of the Policy

16.1 This Policy is the responsibility of the Data Protection Officer, Helen Holmes. She will review the implementation of this Policy regularly considering its suitability, adequacy and effectiveness based upon any report of breaches and/or DSAR's logged and recorded on the Data Map. The Policy will also be reviewed by the COLP and Directors as part of the annual quality review (AQR). Any improvements identified will be made as soon as possible.

The Policy will also be reviewed by the Directors annually as part of the annual quality review which will include a review of any reported or identified Data Breaches, Data Subject Access Requests and a review of timescales for Data Retention, with reference to the firm's Data Map.

16.2 Interpretation:

Automated Decision-Making (ADM):	when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.
Automated Processing:	any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.
Company Personnel:	all employees, workers [contractors, agency workers, consultants,] directors, members and others.
Consent:	agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signify agreement to the Processing of Personal Data relating to them.
Controller:	the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the GDPR. We are the Controller of all Personal Data relating to our Company Personnel and Personal Data used in our business for our own commercial purposes.
Criminal Convictions Data:	means personal data relating to criminal convictions and offences and includes personal data relating to criminal allegations and proceedings.
Data Subject:	a living identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.
Data Privacy Impact Assessment (DPIA):	tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programmes involving the Processing of Personal Data.

Data Protection Officer (DPO):	the person required to be appointed in specific circumstances under the GDPR. Where a mandatory DPO has not been appointed, this term means a data protection manager or other voluntary appointment of a DPO or refers to the Company data privacy team with responsibility for data protection compliance.
EEA:	the 28 countries in the EU, and Iceland, Liechtenstein and Norway.
Explicit Consent:	consent which requires a very clear and specific statement (that is, not just action).
General Data Protection Regulation (GDPR):	the General Data Protection Regulation ((EU) 2016/679). Personal Data is subject to the legal safeguards specified in the GDPR.
Personal Data:	any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Special Categories of Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a

	name, email address, location or date of birth) or an opinion about that person's actions or behaviour. The Company will treat the following types of data as if they are **Special Categories of Personal Data** and this includes, but is not limited to: Client or staff information for which we have a duty of care and responsibility under GDPR names, addresses, matter or case details, salary, information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data. [**DETAILS OF OTHER TYPES OF DATA THE COMPANY CONSIDERS SENSITIVE**]: The Company will treat the following types of data as if they are Special Categories of Personal Data: Files relating to family matters, Files relating to criminal matters, Childcare cases and any information relating to children. Commercially sensitive information. NHS Records. Criminal Records. Business and Company records. Information provided to NCA. Information that is Legally Privileged. HR Data. Individuals bank account or credit card details,
Personal Data Breach:	any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.
Privacy by Design:	implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.
Privacy Guidelines:	any Company privacy and GDPR related guidelines provided to assist in interpreting and implementing this Policy and Related Policies.
Privacy Notices (also referred to as Fair Processing Notices) or Privacy Policies:	separate notices setting out information that may be provided to Data Subjects when the Company collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy) or they may be stand-alone, one-time privacy statements covering Processing related to a specific purpose.
Processing or Process:	any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Pseudonymisation or Pseudonymised:	replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.
Related Policies:	the Company's related policies and procedures or processes related to this policy designed to protect Personal Data.
Special Categories of Personal Data:	information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data. [The Company will treat the following types of data as if they are Special Categories of Personal Data