Data Privacy and Information Management Policy

Contents

1. GENERAL APPROACH TO DATA PRIVACY AND INFORMATION MANAGEMENT

1.1 TWM Solicitors LLP and its associated companies, TWM Trust Corporation Limited and TWM Corporate Services Ltd, (collectively referred to as "TWM") hold a significant amount of confidential information about *Clients, Personnel*, and third parties. We must all comply with data protection law and keep confidential information secure.

1.2 TWM is committed to the highest standards of data protection and information management. This policy sets out TWM's approach to handling the *Personal Data* of our *Clients, Personnel*, suppliers, contractors, contacts, job applicants and other third parties. It includes the precautions we take to keep information secure, which is periodically circulated to Personnel to remind them of their responsibilities. The firm is in the course of obtaining accreditation against Cyber Essentials.

1.3 This Policy applies to all *Personal Data* we *Process* regardless of the media on which that data is stored, whether it relates to past or present *Personnel*, *Clients*, Job Applicants, suppliers, contacts, website users or any other *Data Subject*.

1.4 Please refer to the Glossary in Schedule 1 for the definition of words and expressions used in italics in this Policy.

1.5 TWM has introduced information management systems and information technology to meet its information management needs. We will monitor and where relevant update and improve these systems on a continual basis. The principal systems are case management, library, precedent, intranet and data storage systems.

1.6 Our *Personnel* recognise their individual and collective responsibility to follow relevant practices and procedures in order to maintain day to day excellence in managing and protecting the information entrusted to the practice by our *Clients*, other *Personnel*, job applicants, suppliers, contacts, website users and any other *Data Subject* and to maintain TWM's own information management systems.

1.7 Our *Personnel* will do their best, at all times, to ensure the accuracy, relevance and sufficiency of any information they record in practice files or enter in the firm's systems. They will seek to maintain the quality of this information in accordance with the *Process*es and procedures relevant to their role and they will, at all times, seek to maintain the lawful and proper confidentiality and security of the firm's information assets.

1.8 TWM retains information for the periods set out in Schedule 4. These periods reflect our data protection obligation not to keep personal data for longer than is necessary, and also our statutory, regulatory and business needs to keep records. The firm will review these retention periods at least every five years, or more frequently if there are changes in limitation periods or statutory obligations as to the retention of records.

1.9 Schedule 2 to this Policy sets out the categories of information assets we hold in relation to our *Clients and the lawful basis for doing so*.

1.10 Schedule 3 to this Policy sets out the categories of information assets we hold in relation to *Personnel and the lawful basis for doing so*.

1.11 Schedule 4 to this Policy sets out the categories of information assets we hold in relation to the firm itself, the lawful basis for doing so, and the relevant retention periods.

1.12 Schedule 6 to this Policy sets out the Rights of *Data Subjects.*

1.13 Schedule 7 to this Policy is the TWM privacy notice relating to job applicants.

1.14 Hardware and software assets owned by TWM are recorded and managed through the Inventory system on HR.Net.

1.15 All allocated equipment is assigned to its user and is identifiable by a unique asset tag attached to the equipment.

1.16 Software is managed through *Client* licensing numbers or through the online portal of the software house.

1.17 The majority of the software in use by TWM is from Microsoft and the IT team uses the Microsoft Licensing Portal in conjunction with regular licensing audits from our key supplier.

1.18 TWM reserves the right to update this policy at any time without express notice to any third party, so please check our website regularly for the latest version of this Data Privacy and Information Management Policy. We last revised this document in March 2018.

1.19 This Policy will be reviewed annually in May, or more frequently, as needed, by the Managing Partner/COLP/DPO. Reviews will include considering the data *processing* activities of the firm in light of the obligation of data protection by design and default. A review will also be carried out at the same time of any substantial change in the data *processing* activities of the firm. A data protection impact assessment will be carried out before the firm undertakes processing that may result in high risk to individuals (this is an extremely unlikely scenario and not one that we anticipate ever arising).

1.20 This Data Privacy and Information Management Policy does not override the *GDPR*.

2. PERSONS WITH RESPONSIBILITY

2.1 The person with overall responsibility for this policy is the firm's Managing Partner, Compliance Officer for Legal Practice (COLP) and *Data Protection Officer ("DPO*"), Matthew Truelove. The DPO has overall responsibility for data protection, privacy and information management, and this Policy. Questions on or concerns about these issues should

be referred either to him, to Elizabeth Sewell (the Risk & Compliance Executive), or to your supervising partner.

2.2 Please contact our *DPO* if you have any questions about this Policy or the *GDPR* or if you have any concerns that this Policy is not being or has not been followed. In particular, you should contact the *DPO* or if you are unsure about:

(a) the lawful basis on which you are relying to *Process Personal Data* (including the *Legitimate Interests* used by TWM);

(b) whether you need to rely on *Consent* and/or need to capture *Explicit Consent*;

(c) the retention period for the *Personal Data* being *Processed*;

(d) what security or other measures you need to implement to protect *Personal Data*;

(e) whether you have sufficient legal justification to transfer *Personal Data* outside the *EEA*; and/or

(f) any contracts or other areas in relation to sharing *Personal Data* with third parties (including our suppliers).

2.3 In particular, if you are aware of a *Personal Data Breach* or any other breach of security with confidential information you must report that promptly to Matthew Truelove, Elizabeth Sewell, or the supervising partner. TWM has a duty to report breaches of security to *Clients*, and sometimes to the Solicitors Regulation Authority and/or the Information Commissioner's Office and/or the Solicitors Regulation Authority, and this will be done by Matthew Truelove, the firm's COLP and DPO.

2.4 The following people also have delegated responsibility for data privacy and information management:

Andrew Hayes (Finance)

Kathy Betts (HR)

Alan Barrett (IT)

Georgina Denny (Marketing)

Elizabeth Sewell (Risk & Compliance)

Jamie Berry (Business Law)

Adrian Price (Commercial Property)

Guy Perkins (Dispute Resolution)

Patrick Stewart (Employment)

Sarah Cornes (Family)

Allison Crossman (Private Client)

Stephanie Sharpe (Tax)

Jonathan Potter (Residential Property)

Julian Sampson (Head of Lending)

3. OUR OBLIGATIONS

3.1 When we hold information about identifiable people (known as "*Data Subjects*") this gives rise to obligations under the *General Data Protection Regulation* ("*GDPR*"). The *GDPR* applies whether such information is held in electronic form or in a paper filing system. TWM is a *Data Controller* for the purposes of *GDPR*.

3.2 *Data Subjects* have rights if we hold information about them. That includes the right to be informed what we hold, the right to have errors corrected and the right to have *Personal Data* deleted if we have no justification for holding it.

3.3 We may be liable in various ways if we fail to *Process Personal Data* appropriately. This may include liability in damages for negligence and breach of confidentiality or even criminal liability. We may also be subject to professional sanctions for breach of the SRA Code of Conduct. The following is a summary of our obligations under data protection law, but is not a substitute for full research where appropriate.

4. THE DATA PROTECTION PRINCIPLES

4.1 In *Processing Personal Data*, we must comply with the *Data Protection Principles*, which require that *Personal Data* must be:

(a) *Processed* lawfully, fairly and in a transparent manner;

(b) collected for specified, explicit and legitimate purposes and not further *Processed* in a manner incompatible with those purposes;

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which it is *Processed*;

(d) accurate and, where necessary, kept up to date;

(e) kept in a form which does not permit identification of *Data Subjects* for longer than is necessary for the purposes for which the data is *Processed*;

(f) *Processed* in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful *Processing* and against accidental loss, destruction or damage;

(g) not transferred to a country outside the *EEA* without appropriate safeguards being in place;

(h) made available to *Data Subjects*, who are allowed to exercise certain rights in relation to their *Personal Data*.

4.2 We are responsible for and must be able to demonstrate compliance with the above principles.

5. GROUNDS FOR *PROCESSING PERSONAL DATA*

5.1 We may only *Process Personal Data* if we have a lawful and legitimate justification for doing so.

5.2 The *GDPR* allows *Processing* for specific purposes. Those which most often apply are that the *Processing* is necessary:

(a) for the performance of a contract to which the *Data Subject* is a party, or to take steps at the *Data Subject's* request before entering into such a contract;

(b) for compliance with a legal obligation other than a contractual obligation to the *Data Subject*;

(c) to protect someone's vital interests;

(d) for our *Legitimate Interests*, or those of a third party, where such interests are not overridden by the interests or rights of the *Data Subject*.

5.3 We do not need *Consent* to *Process Personal Data* in any of the cases listed in paragraph 5.2. In other cases, for example, direct marketing (see section 9 below), we may need *Consent*. We will, of course, not usually be contracting directly with anyone under the age of 18, as they will not have legal capacity to enter into contracts but you should note that, for data protection purposes, persons under the age of 13 cannot give a valid *Consent* in their own right, and such *Consent* is required from a parent, or other person holding 'parental responsibility'. We do not ask for *Consent* if we do not need it.

5.4 The *Processing* of *Sensitive Personal Data* is subject to stricter conditions. The usual grounds on which we are entitled to *Process Sensitive Personal Data* are:

(a) *Explicit Consent* of the *Data Subject;*

(b) it is necessary to protect the vital interests of a *Data Subject* who is physically or legally incapable of giving *Consent*;

(c) the *Personal Data* was manifestly made public by the *Data Subject*;

(d) it is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity;

(e) it is necessary for the purposes of carrying out the obligations and exercising specific rights of the *Data Controller* or of the *Data Subject* in the field of employment and social security and social protection law; and/or

(f) it is necessary for occupational health reasons or for the assessment of working capacity of *Personnel.*

5.5 We must ensure that the *Personal Data* we *Process* is accurate, complete, kept up to date and relevant to the purpose for which we collected it. We must do our best to check the accuracy of any *Personal Data* at the point of collection and at regular intervals afterwards and, subject to our overriding legal and professional obligations, we must take all reasonable steps to destroy or amend *Personal Data* which we know to be inaccurate or out of date.

5.6 We must not *Process Personal Data* for purposes other than those for which we originally collected it, unless we reasonably consider that we need to use it for another purpose which is compatible with the original purpose.

5.7 If we need to *Process Personal Data* for a purpose which is new, different or incompatible with that which was disclosed when we first obtained the *Personal Data*, we must inform the *Data Subject*, explain the legal basis which allows us to do so and, in some cases, obtain the *Data Subject's Consent*. Similarly, if the *Data Subject* requires an explanation as to how the *Processing* for the new purpose is compatible with the original purpose, we must provide it.

5.8 Please note, however, that there are many situations where, as solicitors, an employer, or prospective employer, we are required or permitted by law to *Process Personal Data*, in compliance with the above rules, without the knowledge or *Consent* of the *Data Subject*.

6. WHAT PERSONAL DATA WE COLLECT AND HOW WE USE IT

6.1 In Schedules 2 and 3 we have set out a description of the different types of *Personal Data* we may collect, use, store and transfer, the ways we plan to use the *Personal Data*, and the legal justification on which we rely in order to do so. Where we rely on the justification that it is necessary to *Process* the *Personal Data* for our *Legitimate Interests* we have also, where appropriate, identified what we consider those *Legitimate Interests* to be.

6.2 Depending on the specific purpose for which we are *Processing* the *Personal Data*, more than one legal justification may apply. Where more than one legal justification is given in Schedules 2 and 3, *Data Subjects* who require more information about the specific legal justification on which we are relying to *Process* their *Personal Data* may contact us and request an explanation.

6.3 Schedule 7 – Job Applicant Privacy notice – contains a detailed description of *Personal Data* relating to job applicants and how we *Process* that information.

7. TRANSPARENCY

7.1 The *GDPR* requires TWM to provide detailed, specific information to *Data Subjects*, in a concise, transparent, intelligible, and easily accessible manner, and in clear and plain language which can easily be understood. The precise information required depends, among other things, on whether the information was collected directly from *Data Subjects* or from elsewhere. This Policy, and the notice of *Data Subject*'s rights in Schedule 7, seeks to comply with this requirement.

7.2 Whenever TWM collects *Personal Data* directly from *Data Subjects*, including for human resources or employment purposes, we must provide them, when they first provide the *Personal Data*, with all the information required by the *GDPR*, including the identity of the

Data Controller and *DPO*, and how and why we will use, *Process*, disclose, protect and retain their *Personal Data*.

7.3 When *Personal Data* is collected indirectly (eg from a third party or publicly available source), TWM must provide the *Data Subject* with all the information required by the *GDPR* as soon as possible after collecting/receiving the Data. We must also check that the *Personal Data* was collected by the third party in accordance with the *GDPR* and on a basis which contemplates our proposed *Processing* of that *Personal Data*.

8. COOKIES AND OTHER PERSONAL DATA COLLECTION METHODS

8.1 We collect *Personal Data* from and about our *Clients*, contacts, *Personnel*, and other third parties by various different methods, including through:

(a) Cookies, automated technologies or interactions

As users interact with our website, we may automatically collect technical data about their equipment, browsing actions and patterns. We collect this *Personal Data* by using cookies, server logs and other similar technologies.

TWM's website uses cookies to distinguish between users of our website. This helps TWM to provide individual users with a good experience when they browse our website and also allows us to improve our site.

A cookie is a small file of letters and numbers that we store in a user's browser or the hard drive of their computer if they provide their *Consent*. Cookies contain information that is transferred to a user's hard drive.

We use the following cookies:

- Strictly necessary cookies. These are required for the operation of our website. They include, for example, cookies that all users to log into secure areas of our website or make use of e-billing services.

- Analytical/performance cookies. These allow us to recognise and count the number of visitors and to see how visitors move around our website. This helps us to improve the way our website works, for example by ensuring that users can find what they are looking for easily.

We may also receive technical data about our *Clients*, contacts and other third parties if they visit other websites employing our cookies.

TWM uses Google Analytics to collect the above information. These cookies collect information in anonymous form. For further details please visit: https://support.google.com/analytics/answer/6004245

Users can block all or some cookies by adjusting the settings on their browser. However, if they set their browsers to disable or refuse cookies (including essential cookies) users may not be able to access all or parts of our website. To opt out of Google Analytics please visit https://tools.google.com/dlpage/gaoptout

(b) Direct interactions

They may give us their identity, contact and/or financial data by filling in forms, giving us their business card, or by corresponding with us by post, telephone, email or otherwise. This includes *Personal Data* they provide when they:

- become *Clients* of TWM;
- seek information about our products or services;
- create an account on our website;
- subscribe to our service or publications;
- request marketing to be sent to them; and/or
- give us feedback.

In the case of *Personnel* and job applicants this includes *Personal Data* they provide when they:

- apply for work experience or placements within TWM
- apply for a vacancy with TWM
- provide their services to TWM as a consultant
- become an employee or an ex-employee of TWM

(c) Third parties or publicly available sources

We may receive *Personal Data* from various third parties and public sources as set out below:

- Technical Data from parties such as analytics providers, eg Google Analytics based outside the *EEA*; and search information providers eg SmartSearch based inside the *EEA*.
- Contact, financial and transaction data from providers of technical, payment and delivery services such as lending institutions based inside the *EEA*.
- Identity and contact data from publicly availably sources such as Companies House and the Electoral Register based inside the *EEA*.
- Identity, contact, financial data from benefits providers/brokers based inside the *EEA*.
- Identity, contact and financial data from our payroll provider based inside the *EEA*.
- Identity, contact, financial and recruitment data from recruitment agencies and job sites based inside the *EEA*.

9 MARKETING

9.1 We use identity, contact, technical, usage and profile data about our *Clients*, contacts or other third parties to form a view on what we think they may want or need, or what may be of interest to them, and to:

(a) send them occasional newsletters;

(b) tell them about relevant changes in the law;

(c) tell them about services that we provide; and/or

(d) send them invitations;

which we think may be relevant to them.

9.2 We are able to do this without express *Consent* if they have provided us with their Contact Data in the course of a previous instruction, or when requesting information from us about the services we offer so long as we give them an opportunity to opt out of receiving such marketing communications in the first and in each subsequent communication, and they have not done so. Otherwise, we will not send marketing communications to anyone who has not expressly *Consented*.

9.3 We will not share *Personal Data* with any third party for marketing purposes without the express *Consent* of the *Data Subject*.

9.4 *Clients*, contacts and other third parties may ask us to stop sending them marketing communications by contacting us at any time. We must explicitly advise them of their right to do so, in an intelligible manner which is clearly distinguishable from other information.

9.5 If *Clients* or contacts opt out of receiving marketing communications from us at any time, their details will be suppressed as soon as possible. This involves retaining just enough information to ensure that marketing preferences are respected in the future.

9.6 If *Data Subjects* change their mind about receiving marketing communications from us, they can update their choices at any time by contacting us.

10 SHARING *PERSONAL DATA*

10.1 We may have to share *Personal Data* with third parties for the purposes set out in the table in Schedules 2, 3 and 7.

10.2 We will only share the *Personal Data* we hold within the firm if the recipient, in the case of *Client* information, has a matter-related need to know the information or, in the case of *Personnel* and job applicants if managers need to know and the transfer complies with any applicable cross-border transfer restrictions.

10.3 We may need to share *Personal Data* with external third parties, such as:

(a) Service providers, acting as *Process*ors, based within the *EEA* who provide HR and system administration services.

(b) Professional advisers, acting as *Process*ors or joint controllers, including lawyers, bankers, auditors, benefits providers, brokers and insurers who provide consultancy, banking, legal, insurance, pension, healthcare, childcare vouchers, life assurance, and accounting services.

(c) HM Revenue & Customs, regulators and other authorities, acting as *Process*ors or joint controllers, based in the United Kingdom who require reporting of *Processing* activities in certain circumstances.

(d) The Law Society, the Solicitors Regulation Authority, the Legal Ombudsman, Atlantic Data (who *Process Personnel* DBS checks), and Socrates Training Limited (who provide online training).

(e) Banks, other lending/mortgage institutions, lending/mortgage brokers, insurers, and insurance brokers.

(f) Job applicants – please refer to Schedule 7.

10.4 Generally we are not allowed to share *Personal Data* with third parties unless certain safeguards and contractual arrangements have been put in place.

10.5 We will only share the *Personal Data* we hold with third parties, such as our service providers if:

(a) they have a need to know the information for the purposes of providing the contracted services (eg when instructing Counsel, or dealing with TWM's benefits providers/brokers);

(b) sharing the *Personal Data* complies with this Policy and the *Data Subject's Consent*, if required, has been obtained;

(c) the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;

(d) the transfer complies with any applicable cross border transfer restrictions; and

(e) a fully executed written contract that contains *GDPR* approved third party clauses has been obtained or is published on their website.

10.6 We require all third parties to respect the security of the *Personal Data* relating to our *Clients* and to our *Personnel* and to treat it in accordance with the law. We do not allow our third party service providers to use *Personal Data* relating to our *Clients* and to our *Personnel* for their own purposes and only permit them to *Process* such *Personal Data* for specified purposes and in accordance with our instructions.

10.7 A list of our external suppliers, with whom *Personal Data* may be shared, is set out in Schedule 5.

10.8 We may share *Personal Data*, in strict confidence, with third parties with whom we may be contemplating acquiring parts of their business or assets, merging with them or selling, transferring, or merging parts of our business or assets. In such cases, any new owners of the business may *Process Personal Data* in accordance with this Policy.

11 SENDING DATA OUTSIDE OF THE *EEA* (SEE ALSO SECTION 10 - SHARING *PERSONAL DATA*)

11.1 We will only send a *Data Subject's Personal Data* outside of the *EEA* to:

(a) follow a *Client*'s instructions eg their matter involves a foreign property transaction; or a matrimonial matter where the other party or children live in another country;

(b) comply with a contractual, regulatory or legal duty;

(c) work with our agents or advisers who we may use to assist in fulfilling your instructions eg estate agents, Counsel, etc.

11.2 If we do transfer information to our agents or advisers outside of the *EEA*, we will ensure that it is protected in the same way as if it was being used in the *EEA* by putting in place one of the following safeguards:

(a) transferring it to a non-*EEA* country with privacy laws that give the same protection as the *EEA;*

(b) putting in place an agreement with the recipient that means they must protect it to the same standards as is required in the *EEA* or ensuring their existing procedures are compliant; or

(c) transferring it to organisations that are part of Privacy Shield. This is a framework that sets privacy standards for data sent between the US and EU countries. It makes sure those standards are similar to what is used within the *EEA*.

11.3 More information in relation to the points above can be found on the European Commission website.

12 DATA RETENTION

12.1 *Personal Data* must not be kept in an identifiable form for longer than is necessary for the purposes for which the *Personal Data* is *Processed*.

12.2 We must not keep *Personal Data* in a form which permits the identification of the *Data Subject* for longer than is necessary for the legitimate business purpose or purposes for which it was originally collected, or for the purpose of satisfying any legal, accounting or reporting requirements.

12.3 In some circumstances, *Data Subjects* may ask us to delete *Personal Data* we hold relating to them. We do not always have to comply with such requests, and it is not always possible to

do so. In some circumstances we may *Pseudonymise Personal Data* (so that it can no longer be associated with a *Data Subject*) for research or statistical purposes, in which case we may use the *Pseudonymised Personal Data* indefinitely without further notice to the *Data Subject*.

12.4 Schedule 4 to this *Policy* sets out the periods for which *Personal Data* is stored. TWM aims to ensure that, subject to overriding legal and regulatory requirements, *Personal Data* is deleted when no longer reasonably required for the purposes for which it was being held. By law we have to keep basic information about our *Clients* (including Contact, Identity, Financial and Transaction Data) for a minimum of six years after they cease being *Clients*, and often for much longer. Details of our retention timelines are set out in Schedule 4.

12.5 We take all reasonable steps to destroy or erase from our systems all *Personal Data* that we no longer require.

13 *DATA SUBJECT*S' RIGHTS AND REQUESTS

13.1 *Data Subjects* have rights when it comes to how we handle their *Personal Data*. A notice to *Data Subjects* setting out their rights is out in Schedule 6.

13.2 TWM will verify the identity of an individual requesting *Personal Data* under any of the rights listed above and will not allow third parties to persuade us to disclose *Personal Data* without proper authorisation.

13.3 Any written subject access request from someone for information that we hold about them should be forwarded without delay to Matthew Truelove and Elizabeth Sewell. It is their responsibility to consider and record all such requests and respond to them in a timely manner.

13.4 It should be noted that for regulatory, professional indemnity and other professional reasons (eg conflict checking or dealing with any future claims or complaints relating to a *Client*'s matter), we will not delete a *Client*'s matter from the firm's case management and email systems for a minimum of 10 years, and therefore all *Personal Data* provided in order for us to fulfil our *Client*'s instructions will be retained. Non-germane information provided (eg a *Client*'s personal interests or non-relevant family information will be deleted).

13.5 We back up the information held on the firm's computer systems as provided in our Business Continuity Plan. It is not possible to identify *Personal Data* relating to particular *Data Subjects* within such back-ups without restoring the back-up to the firm's system. Only authorised members of the firm's IT Department have access to such back-ups for this purpose.

14 ACCOUNTABILITY

14.1 We have implemented appropriate technical and organisational measures in an effective manner, to ensure compliance with the *Data Protection Principles*. We are responsible for, and must be able to demonstrate, compliance with the *Data Protection Principles*.

14.2 We have allocated adequate resources and put in place sufficient controls to ensure and to document *GDPR* compliance including:

(a) appointing a suitably qualified *DPO* and committee accountable for data privacy;

(b) implementing *Privacy by Design* when *Processing Personal Data* and completing *DPIAs* where *Processing* presents a high risk to rights and freedoms of *Data Subjects*;

(c) integrating data protection into internal documents (including this Policy);

(d) training the firm's *Personnel* regularly on the *GDPR*, information management and privacy, Related Policies and Privacy Guidelines and data protection matters including, *Data Subject*'s rights, *Consent*, legal basis, *DPIA* and *Personal Data Breaches*. TWM maintains a record of training undertaken by our *Personnel*; and

(e) regularly testing the privacy measures implemented, including conducting periodic reviews and audits to assess compliance and assessing the results of this.

15 RECORD KEEPING

15.1 The *GDPR* requires us to keep full and accurate records of all our data *Processing* activities.

15.2 We keep and maintain accurate records reflecting our *Processing*, including records of *Data Subjects' Consents* and procedures for obtaining *Consents.*

15.3 These records include, at a minimum, the name and contact details of the *Data Controller* and the *DPO*, clear descriptions of the types of *Personal Data*, *Data Subjects*, *Processing* activities, *Processing* purposes, third-party recipients of the *Personal Data*, *Personal Data* storage locations, *Personal Data* transfers, the *Personal Data's* retention period and a description of the security measures in place.

16 DATA SECURITY

16.1 All TWM *Personnel* are responsible for the protection and security of information assets entrusted to them. We have identified the following risks to the following categories of information asset along with proposed countermeasures and the member of *Personnel* responsible.

16.2 <u>User accounts</u>

User accounts are set up according to the procedures set out within the new joiner workflow within HR.Net which provides a facility for managers to deal with the joining of new *Personnel*.

TWM's IT team creates a user account and grants access to resources according to these specifications and arranges for the appropriate training to be given.

Alterations to the user account due to a member of *Personnel* relocating between offices or departments are also handled through HR.Net from the mover workflow, while *Personnel* leaving TWM are notified to our IT team who then revoke rights to the VPN and their user accounts on the correct date, collect company equipment from the relevant member of *Personnel*, and redirect telephone and email, thereby ensuring *Client* continuity.

When a request is made at short notice to restrict an account due to a difficult departure, the Head of IT conducts the *Process* on the notification of either a Head of Department or a member of TWM's Executive Committee.

On the absence of *Personnel* at short notice due to illness or some other reason and if a request is made to access that person's data, the IT team will obtain written authorisation from either the line manager, Head of Department or an equity partner before proceeding to grant access to the resource.

Staff responsible for the management of payments (including fee earners, management *Personnel*, and the Finance team) are only assigned to that function after passing suitable background checks, to include verified positive references and a Disclosure and Barring Service (DBS) check (as with all TWM *Personnel*).

16.3 The software in use at TWM is managed by:

(a) Windows Server Update Services ("WSUS") is configured and operated by our IT team to ensure that all systems and applications from Microsoft are up to date. Other applications in use within TWM are on support contracts with the relevant software company and updating and management of such software is carried out in conjunction with their support departments.

(b) SolarWinds, an SNMP based management suite, allows the IT team to monitor system availability and includes monitoring disk space, *Process*or and memory utilisation and other key metrics. The system also notifies the IT team of any issues immediately and allows the production of monthly and annual availability reports which are provided to managers and are the basis of discussion around issue resolution, resourcing and future planning.

16.4 Firewalls

TWM protects its network perimeters with advanced Unified Threat Management ("UTM") appliances, commonly known as firewalls, which are configured according to current best practices and kept up to date s for protection against Trojans, malware, spyware and spam.

The configuration is managed and modified in consultation with an IT consulting business to ensure relevance and best practice is agreed.

The UTM appliances isolate the network into a series of secure virtual domains ("VDOMs") and only TWM prepared equipment may be connected to the Primary VDOM containing the confidential data of the business.

Visitors and employees using their own devices in a "bring your own device" fashion are only allowed to connect to the guest VDOM which has particular UTM rules in place.

All VDOMs are configured to have network traffic captured to an analyser unit and data leak prevention ("DLP") is in place to ensure that records are available both historically and in real time to ensure that the network is secure and events are traceable.

16.5 Network devices

Network devices include: UTM appliances; switches; PBX; physical or virtual servers; ESXi hosts; and workstations.

All network devices are configured according to best practices with regards to security and are tuned up to work as effectively as possible in a dynamic computing environment.

All network devices have their configurations documented and held by the IT team along with procedures for data recovery, upgrade and configuration changes.

We use *Privacy by Design* measures when *Processing* personal data by adopting appropriate technical and organisational measures (such as *Pseudonymisation* and matter passwords) in an effective manner, to ensure compliance with *GDPR*.

16.6 Detection and removal of malicious software

TWM's IT team aims to operate a highly secure computing environment and to prevent infection.

The defence system developed in pursuit of this aim includes, but is not limited to, the following defences:

(a) UTM appliances which are configured to control data flow and inspect all data entering and leaving the network;

(b) Third Party scanning for viruses/malicious code/spam etc within all incoming and outgoing email before or after it enters or leaves the network. This SMTP stream is also inspected at the packet level by the UTM appliances;

(c) Software execution restrictions in place on the thin *Client* computing environment that TWM operates, limiting which executable programs are permitted to be run within the user's sessions;

(d) Anti-virus software provided by Sophos which inspects all written network data for malicious code:

(e) Anti-malware software running within all sessions on thin *Client*; and

(f) Restrictions on data coming in on USB sticks, CD and DVD disks and other portable media which are tested on "Sheep Dip" machines located in each office before being transferred to the network.

16.7 Retention of *Client* information assets

TWM will retain all *Client* information assets indefinitely (subject to periodic review) on the basis that there is tangible advantage to our *Clients* in having access to data that might otherwise be destroyed without chance of recovery.

17 TRAINING

17.2 TWM provides online cyber security, data protection, and information management training to all new *Personnel* on induction and thereafter at least annually. In addition, they are required to read the following TWM policies:

(a) Electronic Systems, Communications and Social Media Policy;

(b) Office Manual and its annexures (comprising all of TWM's policies and procedures);

(c) Anti-Money Laundering Policy.

17.3 The management team periodically circulates emails reminding *Personnel* of current criminal methodologies and risks as well as necessary precautions.

17.4 *Personnel* moving between roles within the firm will receive training in the data privacy and information management *Process*es and procedures relevant to their new role within one week of starting the role.

17.5 All *Personnel* will be alerted to changes in this policy and to changes to any *Process*es and procedures relevant to their current role. If necessary, they will receive further training or guidance in new *Process*es and procedures.

17.6 TWM maintains an awareness programme that reminds all *Personnel* of their key obligations under this Data Privacy and Information Management policy.

18 RESPONSIBILITIES OF TWM PERSONNEL

18.1 Do not collect or use *Personal Data* without a good reason

If *Clients* give us information about themselves this is rarely a problem, as they will usually expect us to record that information and use it for our usual professional purposes. However, take particular care with information about third parties, who may be unaware that we hold information about them. *Personnel* should bear in mind three simple principles:

- Do not record information about people unless it is strictly necessary, and the firm has justification under the grounds set out in this Policy;

- Keep it secure; and

- Delete it promptly when it is no longer needed.

Those principles apply especially to information of an embarrassing, secret or sensitive nature, and where the people concerned have not *Consented* to TWM holding the information.

Personnel may only collect *Personal Data* that they require in relation to their duties: they may not collect excessive data. *Personnel* should ensure any *Personal Data* collected is adequate and relevant for the intended purposes.

Personnel must ensure that, when *Personal Data* is no longer needed for specified purposes, it is deleted or anonymised in accordance with the firm's data retention guidelines.

18.2 Take care when sending personal data to others

Personnel will often need to share *Personal Data* and confidential information with others such as barristers, expert witnesses and other law firms. However before doing so they should consider the following points:

(a) Do they really need the information?

(b) Should documents be redacted so that they do not include irrelevant and unnecessary confidential information?

(c) Can we rely on the recipient to keep the information secure?

(d) Are we sending the information outside the *EEA*? If so *Personnel* should check either that the country in question has been designated by the EU Commission as providing adequate data protection, or that TWM has appropriate contract clauses agreed with the recipient place to protect the data.

(e) In publications and publicity material all *Client* identification information must be removed unless *Clients* have *Consented*.

18.3 Keep papers secure

(a) Keep confidential papers in locked cabinets when they are not in use. If that is not possible, ensure that *Client* and *Personnel* information is not visible. Bear in mind that cleaning *Personnel*, temporary Personnel and others may be present in the building, and that leaving papers where they can be seen risks a breach of security.

(b) Question and, if necessary, redirect or report any stranger you see in an entry-controlled area.

(c) Only take *Client* files (or other confidential information) out of the office when it is absolutely necessary to do so. Take precautions to ensure that such items are not stolen or lost. For example, never leave files in an unattended car.

(d) Be aware that taking paper files out of the office is especially risky. Where possible take information in encrypted digital form, eg on a secure laptop.

(e) Also bear in mind that laptops and other electronic devices may be stolen if taken out of the office. Hence confidential files taken out of the office in electronic form must be encrypted. It is not enough that the machine on which they are stored is password protected. Where possible, when *Personnel* are working out of the office they should access documents over the internet.

(f) *Personnel* must ensure that confidential papers are shredded on disposal.

18.4 Keep IT secure

All *Personnel* must:

- Take care with any email received from an unknown source. Bear in mind that clicking on attachments or links may result in viruses being downloaded.

- Follow TWM's policy on the use of passwords, including the level of complexity, the frequency with which they should be changed, and other precautions such as not writing them down in any form which might be intelligible to a third party. Secure passwords are particularly important with mobile devices, or with logins that would enable people to access the firm's systems remotely.

- Log off from their computer when it is left unattended.

- Ensure that their computer screen does not show confidential information to those who are not authorised to see it. This is particularly important when using a laptop or other device outside the office.

- Ensure that they adhere to TWM's Electronic Systems, Communications and Social Media Policy at all times.

18.5 Take care with payments

TWM has policies in place to protect itself from the risk of funds being diverted. Those responsible for making payments from our bank account receive separate guidance, which includes a strict prohibition on divulging account credentials or security information (including usernames, passwords, PINs and other security codes).

All *Personnel* should be aware of the risk of criminals seeking to divert funds, eg by phone calls or emails to the firm purporting to be from *Clients*, our bank or senior Personnel, or to *Clients* purporting to be from the firm, asking for payments to be made to inappropriate

accounts. *Personnel* must report to their supervising partner, Andrew Hayes (the Finance Director) and/or Matthew Truelove immediately any request they receive for information which might be used to facilitate fraudulent payments.

18.6 Take care when dealing with enquiries

All *Personnel* should*:*

- Beware of "blaggers" (people who attempt to obtain confidential information by deception). This is most commonly done by phone but may also be by email or by calling in person. The following are examples of the precautions all *Personnel* should take when dealing with enquiries.

- Check the identity of the person making the enquiry.

- Check that TWM is authorised by the *Client* (or other relevant person) to pass on this information.

- Ask callers to put their request in writing if unsure about the caller's identity and their identity cannot be checked.

- Refer to the relevant supervising partner for assistance in difficult situations.

- Take particular care with callers who claim to be from our bank. A number of firms have had money stolen from their bank accounts after *Personnel* gave confidential banking information out over the phone.

18.7 Subject Access Requests

TWM may receive a written request (known as a "subject access request") from someone for information that we hold about them. If such a request is received it should be forwarded to Matthew Truelove and Elizabeth Sewell immediately. It is their responsibility to consider and record all such requests and respond to them in a timely manner.

Matthew Truelove

Managing Partner/COLP/DPO

September 2018

SCHEDULE 1

DEFINITIONS OF TERMS USED

***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.

***Client*:** a person or organisation using the services of TWM where that person or organisation has signed or otherwise accepted our Terms of Business.

***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, signifies agreement to the *Processing* of *Personal Data* relating to them.

Data 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 *Data Controller* of all *Personal Data* relating to our Personnel and *Personal Data* used in our business for our own commercial purposes.

Data Subject: a living, identified or identifiable individual about whom we hold *Personal Data*. *Data Subject*s may be nationals or residents of any country and may have legal rights regarding their *Personal Data*.

***Data Protection Officer* (DPO)**: the person required to be appointed in specific circumstances under the *GDPR*.

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*.

Legitimate Interest: the interest of the firm in conducting and managing its business to enable it to give *Clients* the best service and the best and most secure experience. We make sure we consider and balance any potential impact on data subjects (both positive and negative) and their rights before we *Process* their personal data for our *Legitimate Interest*s. We do not use their personal data for activities where our interests are overridden by the impact on them (unless we have their *Consent* or are otherwise required or permitted to by law).

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 *Sensitive 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.

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 your *Personal Data* is a *Personal Data Breach*.

Personnel: all partners, employees, workers, contractors, agency workers, consultants, directors, members, and others.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the *GDPR*.

Process or Processing: 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 ***Pseudonymise***: 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.

Sensitive Personal Data **(now called *Special Categories of Data* in the *GDPR*)**: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual orientation, biometric or genetic data, and *Personal Data* relating to criminal offences and convictions.

SCHEDULE 2

CLIENTS - TYPES OF DATA, AND LEGAL JUSTIFICATION FOR HOW WE USE IT

In the table below, we use the following abbreviations:

Type of Data

1 = **Identity Data** such as first name, maiden name, last name, username or similar identifier, marital status, title, date of birth and gender.

2 = **Contact Data** such as billing address, delivery address, email address and telephone numbers.

3 = **Financial Data** such as bank account and payment card details.

4 = **Transaction Data** such as details about payments to and from the *Client*.

5 = **Technical Data** such as internet protocol (IP) address, login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform and other technology on the devices used to access TWM's website.

6 = **Profile Data** such as interests, preferences, feedback and survey responses.

7 = **Usage Data** such as information about how the user navigates TWM's website.

8 = **Marketing and Communications Data** such as preferences in receiving marketing from us and other communication preferences.

We also collect, use and share aggregated data such as statistical or demographic data for any purpose. aggregated data may be derived from *Personal Data* but is not considered *Personal Data* in law as this data does not directly or indirectly reveal the *Data Subject's* identity. For example, we may aggregate Usage Data to calculate the percentage of users accessing a specific website feature. However, if we combine or connect Aggregated Data with any *Personal Data* so that it can directly or indirectly identify the *Data Subject*, we must treat the combined data as *Personal Data* which will be used in accordance with this Policy.

Legal justification for *Processing*

A = TWM needs to *Process* the data in order to perform the contract we are about to enter into or have entered into with the *Client*.

B = TWM needs to *Process* the data in order to comply with a legal or regulatory obligation.

C = TWM *Process*es the data because it is necessary for our *Legitimate Interest*s (or those of a third party) and the interests and fundamental rights of the *Data Subject* do not override those interests.

Purpose/Activity	**Type of data**	**Legal justification for *Processing* (including basis of *Legitimate Interest*)**
To register the *Data Subject* as a new *Client*	1, 2	A
To *Process* and comply with the *Data Subject's* instructions including: (e) Manage payments, fees and charges (f) Collect and recover money owed to TWM	1, 2, 4, 8	A , C (to recover debts due to us)
To manage our relationship with *the Data Subject* which will include: (g) Notifying the *Data Subject* about changes to our terms or privacy policy (b) Asking the *Data Subject* to leave a review or take a survey	1, 2, 6, 8	A, B, C (to keep our records updated and to study how *Clients* use our products/services)
To enable *Data Subject*s to participate in a prize draw, competition or complete a survey	1, 2, 6, 8	A, C (to study how *Clients* use our products/services, to develop them and grow our business)
To administer and protect our business and our website (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data)	1, 2, 5	B, C (for running our business, provision of administration and IT services, network security, to prevent fraud and in the context of a business reorganisation or group restructuring exercise)
To deliver relevant website content and advertisements to our *Clients* and contacts and measure or understand the effectiveness of the advertising we serve to them	1, 2 5, 6, 7, 8	C (to study how *Clients* use our products/services, to develop them, to grow our business and to inform our marketing strategy)
To use data analytics to improve our website, products/services, marketing, *Client* relationships and experiences	5, 7	C (to define types of *Clients* for our products and services, to keep our website updated and relevant, to develop our business and to inform our marketing strategy)
To make suggestions and recommendations to *Data Subject*s about products or services that may be of interest to them	1, 2 ,5, 6,7	C (to develop our products/services and grow our business)

SCHEDULE 3

PERSONNEL - TYPES OF DATA, AND LEGAL JUSTIFICATION FOR HOW WE USE IT

Type of Data

1 = **Identity Data** such as first name, maiden name, last name, username or similar identifier, marital status and dependents, title, date of birth and gender, national insurance number, passport, birth certificate or other Right to Work documentation, driving licence, MOT, insurance documents, and photographs.

2 = **Contact Data** such as address, email address and telephone numbers including next of kin and emergency contact.

3 = **Financial Data** such as bank account and payroll records including tax and NI status, salary, payments to pension providers, childcare voucher providers, cycle to work scheme, incentive payments, overtime payments, expenses, benefits in kind and season ticket loans.

4 = **Recruitment records** such as, references and other information included in a CV or cover letter or as part of the application *Process*.

5 = **Employment records** such as offer letters, contracts of employment, written particulars, DBS checks, SRA and Law Society qualification and disciplinary checks, start and leaving dates, job titles, location of employment or workplace, work history, working hours, annual leave, performance reviews, disciplinary and grievance records, training records, professional memberships, death benefit nomination forms, resignation and termination letters, working time opt-outs and maternity/paternity leave records.

6 = **Security Data** such as CCTV footage and other information obtained through electronic means such as swipe-card records.

7 = **Special Categories of *Sensitive Personal Data*** such as information about race or ethnicity, religious beliefs, sexual orientation and political opinions, health (including any medical condition, health and sickness records, genetic information and biometric data), and criminal convictions and offences. To clarify, TWM will use information relating to leave of absence, which may include sickness absence or family-related leave, to comply with employment and other law. TWM will use information about physical or mental health, or disability status, to ensure a *Data Subject's* health and safety in the workplace and to assess their fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits. TWM will use information about a *Data Subject's* race or national or ethnic origin, religious, philosophical or moral beliefs, or moral beliefs, or sexual orientation to ensure meaningful equal opportunity monitoring and reporting. TWM does not need a *Data Subject's Consent* if special categories of their *Personal Data* are used in accordance with our written policy to carry out our legal obligations or exercise specific rights in the field of employment law. In limited circumstances, TWM may approach a *Data Subject* for their written *Consent* to allow the firm to *Process* certain particularly *Sensitive Personal Data*. If we do so, the *Data Subject* will be provided with full details of the information that TWM would like and the reason it is needed, so that the *Data Subject* can consider whether they wish to *Consent*. The *Data Subject* should be aware that it is not a condition of their contract with TWM that they agree to any request for *Consent*.

8 = **Technical Data** such as information about use of our information and communications systems, internet protocol (IP) address, login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform and other technology on the devices used to access our website.

9 = **Profile Data** such as username and password, interests, preferences, diversity information.

10 = **Accident Records**

Legal justification for *Processing*:

A = TWM needs to *Process* the data in order to perform the contract we are about to enter into or have entered into with the *Client*.

B = TWM needs to *Process* the data in order to comply with a legal or regulatory obligation.

C = TWM *Process*es the data because it is necessary for our *Legitimate Interests* (or those of a third party) and the interests and fundamental rights of the *Data Subject* do not override those interests.

Purpose/Activity	**Type of data**	**Legal justification for *Processing* (including basis of *Legitimate Interest*)**
Making a decision about recruitment/appointments, and determining the terms on which a *Data Subject* will work for the firm	1, 2, 3, 4	A
Checking a *Data Subject* is legally entitled to work in the UK	1, 2, 4	B
Paying *Data Subjects* and, in the case of *Personnel*, deducting tax and National Insurance contributions, applying salary sacrifice adjustments.	1, 2, 3	A, B
Paying *Data Subject's* expenses	1, 3	A
Providing the following benefits to *Personnel*: Healthcare, Life Assurance, Childcare Vouchers, Employee Assistance Programme, Travel Loans, Cycle to Work scheme, Dental benefits	1, 2, 3	A, B
Liaising with *Data Subject's* pension provider and broker	1, 2, 3 (and 4 in regard to healthcare and life assurance)	A
Administering the contract entered into the *Data Subject*	1,2,3,4,5,6,7,8, 9	A, B, C

Purpose/Activity	**Type of data**	**Legal justification for *Processing* (including basis of *Legitimate Interest*)**
Business management and planning, including accounting and auditing.	1, 3, 5	A, B
Conducting performance reviews, managing performance and determining performance requirements.	1, 5, 6, 7, 8	A
Making decisions about salary reviews and compensation.	1, 3, 5	A
Assessing qualifications for a particular job or task, including decisions about promotions	1, 5	A
Gathering evidence for possible grievance or disciplinary hearings	1, 4, 5, 6, 7, 8	A
Making decisions about a *Data Subject's* continued employment or engagement	1, 4, 5, 6, 7, 8	A
Making arrangements for the termination of the working relationship	1, 4, 5, 6, 7, 8	A, B
Education, training and development requirements	1, 4, 5	A
Dealing with legal disputes involving employees, workers and contractors, including accidents at work.	1, 3, 4, 5, 6, 8	A, B
Ascertaining a *Data Subject's* fitness to work and managing sickness absence	1, 2, 4, 5, 6, 7, 8	A, B
Complying with health and safety obligations	1, 2, 6, 7, 10	A, B
To prevent fraud	1, 2, 3, 4, 5, 6, 7, 9	A, B
To monitor *Data Subject*s' use of the firm's information and communication systems to ensure compliance with IT policies.	1, 8	A
To ensure network and information security, including preventing unauthorised access to the firm's computer and electronic communications systems and preventing	1, 8	A

Purpose/Activity	**Type of data**	**Legal justification for *Processing* (including basis of *Legitimate Interest*)**
malicious software distribution.		
To conduct data analytics studies to review and better understand employee retention and attrition rates.	1, 3, 5, 8, 9	C
Equal opportunities monitoring	1 (promotions only), 4, 7, 9	B - SRA compliance

SCHEDULE 4

INFORMATION ASSETS HELD BY TWM AND RELEVANT RETENTION PERIODS

Information Asset	Firm or Client Asset?	Hard Copy or Electronic	Location	Back-up arrangements	Retention Schedule	Oustanding Risk?	Grounds for *Processing* Personal Data Usually Relied On	Privacy Notices in Place?	Any Action Required
Deeds, wills and other original client documents	Client	Hard copy	Wills scanned and stored at Kellys.	Client records for Wills are kept on HR.Net technical solution with SQL. SAN is backed up to tape on a GFS rotation. Email archive is an outsourced solution.	Indefinite	No	Consent of the *Data Subject*. Contractual necessity. Necessary for compliance with a legal obligation. Necessary to protect the vital interests of data subject or another. Necessary for legitimate interests of *Data Subject* or other. Necessary under employment law. Necessary for conduct of legal claims.	Yes.	
Client files (paper)	Mixed	Hard copy	Current files: filing cabinets in offices. Old files are stored with Kellys.	None.	Files will be destroyed after 10 years, except for commercial / residential purchase files which are retained for 15 years. Wills and Deeds are retained indefinitely or until requested by client or their executor.	Possible risk of documents being lost or destroyed.	Consent of the *Data Subject*. Contractual necessity. Necessary for compliance with a legal obligation. Necessary to protect the vital interests of *Data Subject* or another. Necessary for legitimate interests of subject or other. Necessary under employment law. Necessary for conduct of legal claims.	Yes.	Fee earners to be reminded of need to ensure that scanned copies of original contracts, evidence etc is retained on the intranet, by COLP.
Client files (electronic): emails, drafts etc.	Mixed	Electronic	PMS, SQL, SAN, Exchange server and email archive	SQL and Exchange VMs are backed up nightly. SAN is backed up to tape on a GFS rotation. Email archive is an outsourced solution.	VMs - 30 days. SQL databases - first back up of the month held for 2 years, GFS rotation to tape held on tape for first back up of the month indefinitely and email archive kept for 7 years. Tapes held in fire safe.	No. All data on the system is backed up by one or more of a number of methods.	Ditto	Yes.	(1) Fee earners to be reminded of the policy that documents to be stored only per the firm's policies. (2) Fee earners to be reminded of need to redact irrelevant personal data when sharing due diligence information with third parties during corporate transactions. (3) Similar warning to be

Information Asset	Firm or Client Asset?	Hard Copy or Electronic	Location	Back-up arrangements	Retention Schedule	Oustanding Risk?	Grounds for *Processing* Personal Data Usually Relied On	Privacy Notices in Place?	Any Action Required
									given to litigators about redaction of disclosure documents in litigation. Reminder by COLP.
Client identification and verification information (copies of passports, utility bills, driving licence etc) under money laundering regulations. Generally, information obtained from clients would include: full names; marital status; date of birth; gender; billing, delivery and email addresses; telephone numbers; financial data including bank account and payment card details; and transaction data (includes payments to and from *Data Subject)*	Firm	Electronic	PMS and on SAN in unstructured format	SQL and Exchange VMs are backed up nightly. SAN is backed up to tape on a GFS rotation. Email archive is an outsourced solution.	Legal minimum retention period is five years from the end of the client relationship. In practice kept 10 years to allow for fresh instructions, with consent of clients, obtained at time of instruction. Also retained for conflict checking and professional indemnity reasons.	No	Consent of the *Data Subject*. Contractual necessity. Necessary for compliance with a legal obligation.	Yes.	
Records of internal anti-money laundering notifications and Suspicious Activity Reports	Firm	Mixed	Folder maintained by MLRO.	SAN back up	Indefinite	Precautions are in place to ensure only authorised personnel can access	Contractual necessity. Necessary for compliance with a legal obligation.	Yes.	
Database of present and former clients	Firm	Electronic (since 2003)	PMS and on SAN in unstructured format	SQL and Exchange VMs are backed up nightly. SAN is backed up to tape on a GFS rotation. Email archive is an outsourced solution.	VMs - 30 days. SQL databases - first back up of the month held for 2 years, GFS rotation to tape held on tape for first back up of the month indefinitely and email archive kept for 7 years. Tapes held in fire safe.	No	Consent of the *Data Subject*. Contractual necessity. Necessary for compliance with a legal obligation.	Yes.	

Information Asset	Firm or Client Asset?	Hard Copy or Electronic	Location	Back-up arrangements	Retention Schedule	Oustanding Risk?	Grounds for *Processing* Personal Data Usually Relied On	Privacy Notices in Place?	Any Action Required
Claims and complaints files	Firm	Mixed	Riliance, secure/confidential drive, and hard copies kept in locked cabinets	Per appropriate IT measures set out elsewhere in this schedule.	Closed claims and complaints are retained indefinitely at Kellys.	No	Consent of the D*ata Subject.* Contractual necessity. Necessary for compliance with a legal obligation. Necessary to protect the vital interests of *Data Subject* or another. Necessary for legitimate interests of *Data Subject* or other. Necessary for conduct of legal claims.	Yes.	
File review records	Firm	Mixed	Server, matter files and management files kept in lockable cabinets.	Soft copies per appropriate IT measures set out elsewhere in this schedule.	Hard copies destroyed after 12 months.	No	Consent of the data subject Contractual necessity. Necessary to protect the vital interests of *Data Subject* or another. Necessary for legitimate interests of subject or other.	Yes.	
Firm management records, including insurance, property, partnership information, contracts with suppliers.	Firm	Mixed	Server (secure drives) and management files kept in lockable cabinets	Soft copies per appropriate IT measures set out elsewhere in this schedule	Indefinitely	No		Yes	

Information Asset	Firm or Client Asset?	Hard Copy or Electronic	Location	Back-up arrangements	Retention Schedule	Oustanding Risk?	Grounds for *Processing* Personal Data Usually Relied On	Privacy Notices in Place?	Any Action Required
HR records including but not limited to: job applications, current staff records, appraisal data, practising certificate applications, former staff records, pensions and benefits information, National Insurance and tax information, disciplinary and grievance, contracts, driving documents, maternity/paternity leave documentation, and absence records.	Firm	Mixed	HR.Net, ADP, HR Drive, various paper files locked in HR cupboards		6 months from receipt if an unsolicited job application (except for unsolicited agency CVs which are not retained) or 1 year from the date the vacancy is filled, and 18 months for shortlisted trainee applications. 10 years - Former staff records, including disciplinaries and grievance information (spent disciplinaries are disregarded after 6 months for 1st written and 12 months for 2nd written warnings); NI/tax/salary records; Sickness and general absence records including maternity / paternity / parental; and redundancy details.	No	Consent of the *Data Subject* where applicable. Contractual necessity. Necessary: for compliance with a legal obligation; for legitimate interests of data subject or another individual; for conduct of legal claims; under employment law; and to protect the vital interests of the data subject or another individual.	Yes	
Financial records including time recording data, bank data, accounts, payroll, VAT, PAYE, accountant's reports.	Firm	Mixed	HR.Net, ADP, HR Drive, various paper files locked in HR cupboards		10 years: Payroll records and bank details	No	As above.	Yes	
Health and safety certificates.	Firm	Mixed	HR Drive. H&S files locked in HR cupboards		3 years from date of last entry - Accident Books/Accident Reports/records/First Aid and Fire Warden certificates. Other Health & Safety Certificates - permanently	No	As above.	Yes	

Information Asset	Firm or Client Asset?	Hard Copy or Electronic	Location	Back-up arrangements	Retention Schedule	Oustanding Risk?	Grounds for *Processing* Personal Data Usually Relied On	Privacy Notices in Place?	Any Action Required
Files and information held in respect of predecessor, merged and acquired practices	Firm	Mixed	Papers retained in locked cabinets. Electronic data retained in SQL database and SAN in unstructured format	SQL and SAN back up regime as above.	VMs - 30 days. SQL databases - first back up of the month held for 2 years, GFS rotation to tape held on tape for first back up of the month indefinitely and email archive kept for 7 years. Tapes held in fire safe.	No	As above.	Yes	
Register of IT and other equipment owned by the firm.	Firm	Electronic	SQL database and supplier portals	SAN back up	SQL database regime	No	As above.	Yes	
Marketing materials including logos, brochures and other design work, marketing database, Constant Contact, client feedback and testimonials etc.	Firm	Mixed	Outlook, shared drive, electronic	Soft copies per appropriate IT measures set out elsewhere in this schedule	Indefinite. *Data Subjects* can update their marketing preferences at any time.	No	Consent of the *Data Subject* where applicable, and marketing preferences can be updated at any time via published methods. Actioned within 2 working days.	Yes	Training at local level required to flag and remove contacts. Information to be published on the intranet on where to direct these queries.
Website - IP addresses	Firm	Electronic	Outlook		Email archive	These are stored on the website CMS also, so DDA currently has access to these via secure log-in	These are website enquiry forms directed to relevant fee earner to action. We store cookie information to understand browsing patterns and history, and we use IP address to identify generic location information eg town. We do not have specific street address etc.	Yes	

SCHEDULE 5

EXTERNAL SERVICE PROVIDERS

Name of supplier	Description
2i	Recruitment agency
A J L Percy	Consultant Orthopaedic Surgeon
Accurate Data - US Bankruptcy Search	Tracing Beneficiaries
Accuro Transcription Services Ltd	Dictation transcription
Acorn Court	Home Care/Nursing Homes
Acquis Accountancy	Accountant
ADP	Payroll
Advanced Legal	Evolution, AlphaLaw and Laser Forms Hub
Aegon	Group personal pension providers
AIMS Accountants	Accountant
Alan Greenwood & Sons	Funeral Services
Alistair Hodge	Estate Agents
Anna Rabin	Business Law consultant
Answers Investigation	Process Server/Enquiry Agent
Anthony Taylor - Taylor Forrest	Chartered Surveyors
AppDome	Trial status: Fuse APK technology
Ashley Park Nursing Home	Home Care/Nursing Homes
Ashtead Hospital - Martin Bricher	Ashtead Hospital
Ashton Funeral Services	Funeral Services
Ashville Knight	Recruitment agency
Aspin Analysis Ltd	Independent Financial Adviser
Atlantic Data	DBS checking service
Austin Lloyd	Recruitment agency
B Davis Coulthards	Accountant
Badgemaster	TWM badges
Baker Tilly	Accountant
Barbara Martin & Co	Accountant
Barclays Bank plc	Banking
BDO LLP	Accountant
Bellmans	Auctioneers/Valuers
Bells Commercial Ltd	Chartered Surveyors
Bentley Executive	Recruitment agency
Bespoke Legal	Recruitment agency
Bickers Insurance Services	Insurers of Empty Property
BigHand	Digital dictation
Birdscroft Nursing Home	Home Care/Nursing Homes
Birtley House Nursing Home	Home Care/Nursing Homes

Blackberry	Mobile phone management platform
Blue Pelican	Recruitment agency
Bonhams	Auctioneers/Valuers
BPP	Training
Brewers	Accountant
Brian Gale Surveyors - Brian Gale	Surveyor and LPA Receiver
Bristow Burrell	Accountant
Bryden Johnson	Independent Financial Adviser
Bullimores LLP	Accountant
Bundledocs	Trial Status: Online service to create bundles
BUPA	Private healthcare
Burns & Webber	Estate Agents
Butterfield Private Bank	Independent Financial Adviser
C & N Lawrence	House Clearance
Care Asset Management	Independent Financial Adviser
Care Fees Investment Ltd	Independent Financial Adviser
Caterham Clearance Centre	House Clearance
CCH	Tax and trust software
Cedar Court Care Home	Home Care/Nursing Homes
Central Law Training	Training
Certainty	Searches missing wills
CG Legal Training	Training
Chadwick Nott	Recruitment agency
Chalkmead	Home Care/Nursing Homes
Chambers and Partners	Legal directory
Chancel Liability Service	Searches
Chantries	Estate Agents
Charles Stanley & Co	Independent Financial Advisers / Stockbrokers
Charterhouse	Provider of mobile phone contracts
Chris Hall Car Sales	Car Sales - Probate Valuations
Christian Reid	Estate Agents
Christine Hogan	Temporary secretarial services
Christopher Calver Groom	Independent Financial Adviser
Christopher Stone Valuations	Auctioneers/Valuers
Chronicall	Software analysis for Rekoop
Civil & Commercial Costs Lawyers Ltd - Andrew MacKenzie	Costs Draftsmen
Cladding Consultancy Services - Brendan Donoghy	Building Surveyor / Building Engineer
Claire Edwards Eldercare Consultant	Consultant
Class Telecom	Provider of landlines and support on PBX
Clearance Solutions Limited	House Clearance
CNG Inc	Auctioneers/Valuers
Coffee At Work	Vending machine
Colin J Read	Consultant Orthopaedic and Trauma Surgeon
Colin Short	Aircraft Engineer

Companies House	Searches
Conneely Tribe - Austin Marshall	Chartered Surveyors
Constant Power Supply	Maintenance of UPS to server rooms
Country Cousins	Home Care/Nursing Homes
County Enforcement Group	Enforcement Agents
Cranleigh Funeral Services	Funeral Services
Crow Watkin	Estate Agents
CSL Partnership	Accountant
Cyber Insurance (Locktons)	Cyber Insurance wirh Support Services
Davenport Financial Management	Independent Financial Adviser
Davina Hyde	Temporary secretarial services
Dawkins Specialist Civil Enforcement Agents	Enforcement Agents
Dawn Jageurs	Locum
Dell EMC	Supplier of SAN and servers
Delva Patman Associates - Alistair Redler	Rights of Light / Party Wall Act / Boundary Determination
Denhams	Auctioneers/Valuers
Diamond Logistics	Couriers
Direct Design	Website, intranet and print
DMS	Process server/enquiry agent
Douglas & Co	Estate Agents
Douglas Scott	Recruitment agency
Dr M Sharma	Medical Professional
Dr Philip Hall	Medical Professional
Dr R Jacoby	Medical Professional
Dr Saad Khalaf	Medical Professional
Dr Y Sokan	Medical Professional
Dungate Manor	Home Care/Nursing Homes
eBuyer	Supplier of hardware
Edenred	Childcare vouchers provider
EE	Mobile phone service
Effortless Relocation	House Clearance
EFG Harris Allday	Stockbrokers
Egress	Virtual data rooms
EH Solutions	Health and Safety Consultant
Ellisons	Estate Agents
Emerald Colour	Design, print
Emma Ayling	Training
Epsom Beaumont	Home Care/Nursing Homes
Epsom Stamp Company	Auctioneers/Valuers
Esprima	Training
Essendex	Bulk texting service
European Wealth	Stockbrokers
Everycare (East Surrey) Ltd	Home Care/Nursing Homes
Ewbanks	Auctioneers/Valuers
Experian	Unclaimed assets register searches

Exponential-e	WAN and internet connectivity services
Facebook	Social media software
FastSigns	Print, signature
Financial Profiles	Independent Financial Adviser
Finlays Bureau & Investigation Ltd	Process server/enquiry agent
Flexilaw Ltd	Locum
Fonebanker	Disposal of old mobiles
Foolish-IT	Crypto prevent software
Formedecon Limited - Andrew Stephens	Signature Analysis
Fortinet	Firewall appliances
Forum Wealth Management	Independent Financial Adviser
Foxtons	Estate Agents
FPD Savills	Estate Agents
FPSS	Accountant
Frankham Consultancy Group - Chris R P Gibbs	Civil Engineer
Fraser & Fraser	Tracing Beneficiaries
Fuller Gilbert	Estate Agents
FW Paine	Funeral Services
G E Fulton & Son	Auctioneers/Valuers
Gascoigne Pees	Estate Agents
Gatwick Diamond Investigations	Process server/enquiry agent
GDK	Air conditioning services
Gem & Co	Independent Financial Adviser
Gibson Hewitt & Co - Lynn Gibson	Insolvency Practitioner
Gidden Place	Printing
Global Networks Intl Ltd	Provider of PBX and lines
Go Daddy	Certificate services
Google+	Social media software
Graham Randall	Building Surveyor
Grayside Financial Services	Independent Financial Adviser
Haart	Estate Agents
Hailsham Cellars	Branded Champagne
Hakim Fry	Accountant
Halliwell Marks	Estate Agents
Hamlin Iles & Crago - Simon Crago	Building Surveyor
Hamptons International	Estate Agents
Hardware.com	Network switch warranty and support
Harris & Harris	House Clearance
Hartley Fowler LLP	Accountant
Hawes & Co	Estate Agents
Hays	Recruitment agency
Hazel Mead	Temporary receptionist services
Hazlewoods LLP	Accountants/Auditors
Headline Design & Print	Print
Health and Safety Laboratory - Matthew Birthles	Ergonomist

Heimdal	Software and service for anti-malware and DNS poisoning
Helmores UK	Accountant
HFS Milbourne	Pensions and group life assurance broker / IFA
High Court Enforcement Group Ltd	Enforcement officer
High Court Solutions	Enforcement Agents
Hill Clements	Estate Agents
HJP	Independent Financial Adviser / Stockbroker
Holborn Financial Ltd	Independent Financial Adviser
Holly Digital	Printers
Hootsuite	Social media software
Host Logic	IT consultant
Huggins, Edwards & Sharp	Surveyor / Valuer / Property Management
Hurley Partners Limited	Independent Financial Adviser
Ian Caldwell	Auctioneers/Valuers
Ibbett Mosely	Estate Agents
ICU Investigations Ltd	Process Server/Enquiry Agent
IJ Beim Associates	Process Server/Enquiry Agent
Informed Choice	Independent Financial Adviser
Infosec	Security Awareness Training Provider
Intapp	Rekoop, time recording data held in cloud
Investec	Independent Financial Adviser
Isokon	Private Client software provider
ITC Secure	Cyber Security Consultancy
ITS Legal Services	Enquiry Agent
James Insurance Services	Insurance brokers
James Mitchell	House Clearance
Jennifer Gooding	Temporary receptionist services
JMC Legal	Recruitment Agency
Joe Lambe	Auctioneer / Valuer / House Clearance
John D Wood	Estate Agents
John M Hayes Partnership	Costs Draftsman
John McCann	Estate Agents
John W Dall - James Flynn (Chartered Surveyors)	Valuer
Jon S Wand - Chelenham Hospital	Consultant Orthopaedic Surgeon
Jordans Ltd	Identity checking
Jude Mordi	Temporary locum
Karen Crook	Employment Law consultant
Keeley's Kitchen	Catering
Kent Financial Services - Adrian Kent	Tracking and Status Report
Kingston Smith LLP	Forensic Accountant
Kinleigh Folkard & Hayward	Estate Agents
Knight Frank	Estate Agents
Knowle Park Nursing Home	Home Care/Nursing Homes
Knox Bros	Funeral Services
Kutana	Software for Print

L Hawkins & Sons	Funeral Services
Lan2Lan	Firewall subscriptions and support
Land Registry	Property
Cullen & Co - Lauren Cullen	Insolvency Practitioner
Law Absolute	Locums
Law Costs Draftsman - Paul Lavender	Costs Draftsmen
Lawrences	Auctioneers/Valuers
Legal & Public Notices Advertising Agency	Agents - s27 Trustee Act Notices/Advertisements
Legal 500	Legal directory
Legal Connect	Conference call provider
Legastat Ltd	Documentation and Disclosure Support
Lender Exchange	Panel management
Lexis Nexis	Publications
LinkedIn	Social media software
Lloyds Bank plc	Bank
LMS	Lender Panel Management
Lockton Companies LLP	Insurance brokers
London Data Cabling	Provide network cabling
London House Services	Process Server/Enquiry Agent
Longhurst	Funeral Services
Louise Connolly	Family consultant
Love Your Logo	Promotional items
LPC Law	Advocacy Service
LR Legal	Recruitment agency
Ludlow Thompson	Estate Agents
M Spigelman	Consultant Orthopaedic Surgeon
Macdonald Detteiler	Searches
Madasans	Process Server/Enquiry Agent
Mandeep Ryatt	Locum
Mann Countrywide	Estate Agents
Marc Borgia	Tracing Beneficiaries
Mary Cumberlege	Temporary secretarial services
Mason & Ball Services Ltd	Independent Financial Adviser
Matt Pereira Photography	Photography
Matthew Solan - Surrey Foot & Ankle Clinic	Consultant Orthopaedic Surgeon
Medico-legal - John Scurr	Consultant Surgeon
Menzies	Independent Financial Adviser
Menzies	Accountant
MFS	Independent Financial Adviser
Michael Everett	Estate Agents
Microsoft	Software
Milner House	Home Care/Nursing Homes
Mimecast	Email filtering and archiving
Moore Probate Research	Tracing Beneficiaries
Motus	Recruitment agency

MRS Costs Solicitors	Costs Draftsmen
MSP Secretaries	Company Formation
Murdoch Asset Management	Independent Financial Adviser
Neustar UltraDNS	DNS Services for domain names
Nick Bond Photography	Photography
Nuffield Care Centre	Home Care/Nursing Homes
Oades - Simon Worthington	Outdoor clerk and process server
Oakhurst Court	Home Care/Nursing Homes
Oakwood Consultants	Accountant
OG Solutions	Stationery, office supplies and furniture
Ogier	Advice in Jersey
Omell Associates (Fine Art)	Auctioneers/Valuers
Orange Promotions	Branded promotional items
Orpwood Associates Ltd - Trevor Orpwood	Building Surveyor
Oyez	Court Forms
Patrick Gardner & Co	Estate Agents
Paul Dyer	Building Surveyor
Paxton	Security system manufacturer
Penhaligan Recruitment	Recruitment agency
Peter Libby	House Clearance
Peter McCullough	Locum
Peter Tuskin	Locum
Pewleys	Estate Agents
Philip J Orr	Accountant
PHM Ltd	Life assurance broker
Pimms Funeral Services	Funeral Services
Pitney Bowes	Franking machine supplier
Planet Domain	Registry for TWM's domain names
Pole Structual Enginieers - Simon Pole	Engineer
Positive Solutions	Independent Financial Adviser
Price Ferguson	Stockbrokers
Probate Support Services	Registrars
Professor Robin Jacoby	Old Age Psychiatry
Progressive Legal Training	Training
Proofpoint	Cloud based archiving service for emails
PT Legal	Recruitment agency
Pure360	Email marketing platform
QED	Recruitment agency
Quinton Scott Ltd	Surveyor / Estate Agent
Radley Forensic Document Laboratory Ltd - Robert Radley	Forensic Accountant
Rajesh Sapra	Locum
Rayment Matthews & Johnson	Independent Financial Adviser
Reed	Recruitment Agency
Reigate Beaumont	Home Care/Nursing Homes

Reigate Quaker HA	Home Care/Nursing Homes
Rekoop	Digital time recording provider
Re-Tek	Recycling service for old equipment
Ridgegate	Home Care/Nursing Homes
Risk Assurance Management	Group life assurance provider
Robert Holmes & Co	Estate Agents
Robert Leech	Estate Agents
Roffe Swayne	Accountant
Roger Coupe	Estate Agents
Romans	Estate Agents
RR Paice & Co - Robin Paice	Building Surveyor
RSM - Guy Jackson	Insolvency Practitioner
Rutland House	Home Care/Nursing Homes
Safari	Online technical book subscription
Sarah Watson	Temporary secretarial services
Savills Commercial Limited - Alastair Stimson	Valuer
Search Acumen	Search Provider
Search Flow	Local authority searches
Selectamark	Asset tags
Sense Studio Limited - Michael Clift	Architect
Senseco	Environment sensing in main server room
Seymours	Estate Agents
Shipleys	Accountant
Shoppers Anonymous	Mystery shopping
Shred-on-Site	Shredding
Sigma Asset Management	Independent Financial Adviser
Sixty Plus	Independent Financial Adviser
Smart Search	Anti-money laundering checks
Smart Security	Door security and CCTV
SMART4 Limited - Ian Rusbridge	Planning Consultant
Smith & Williamson	Business Valuation / IFA
SMProcess	Enforcement Agents
Socrates Training Ltd	Training
SoftCat	Software and consultancy services
SolarWinds	SNMP monitoring software
Sophos	Anti-virus scanning software
Spackman Accountancy	Accountant
Spink (coin valuers)	Auctioneers/Valuers
ST Johns Ambulance	Fire Warden and First Aider training
Stiles Harold Williams - Alex Gould	Building Surveyor
Stoneman Funeral Service	Funeral Services
Sunrise Senior Living	Home Care/Nursing Homes
Super Anti SpyWare	Software scanning for anti-malware
SW19	Estate Agents
Symantec	Back-up software

Symprex	Email signature management software
Tate	Recruitment agency
Taylor Root	Recruitment agency
TCE Limited	TWM enamel badges
Team Q	Office maintenance
Tendacare	Home Care/Nursing Homes
The Giles Document Laboratory - Dr Audrey Giles	Forensic Scientist
The Lawyer – UK 200	Legal directory
The Notary Practice	Agent
The Old Rectory Nursing Home	Home Care/Nursing Homes
The Personal Agent	Estate Agents
The Property Search Group	Searches
The Red House	Home Care/Nursing Homes
The Sheriff's Office	Enforcement Expert
Thesis	Stockbrokers
Thesis Asset Management	Independent Financial Adviser
THIG	Private healthcare broker
Tiltwood	Home Care/Nursing Homes
Title Research	Searches / Tracking Beneficiaries
Towry	Independent Financial Adviser / Stockbroker
Tpower Solutions Limited	Tracking Agent
Travelers Insurance Co Ltd	Insurance
Tree Surveys - Simon Holmes	Arboriculturalist
Tremark Associates Ltd	Process server/enquiry agent
TSF Consultants	Medical Professional
Twitter	Social media software
ULS	Lender Panel Management
Vanstones	Estate Agents
Veeam	Back-up software for virtual machines
Venn Group	Locums
Verisign	Digital certificate signing
Vestra Wealth LLP	Independent Financial Adviser / Stockbroker
Vista Partners Limited	Independent Financial Adviser / Accountant
W A Truelove & Son Ltd	Funeral Services
Watchman	Insurers of Empty Property
Watkins Oram Limited	Vehicle insurance brokers
Web Results Direct	Search engine optimisation
Westcott House	Home Care/Nursing Homes
White & Sons	Estate Agents
Wilkins Kennedy	Accountant
Williams & Co	Accountant
Williams de Broe Ltd	Independent Financial Adviser
Woodlands	Estate Agents
Woollens	Estate Agents
Worplesdon View Care Home	Home Care/Nursing Homes

Wray Common Nursing Home	Home Care/Nursing Homes
Wray Park	Home Care/Nursing Homes
Wrightman Plans	Plan Draughtsmen
WSM	Accountant
Wykeham House	Home Care/Nursing Homes
Zerto	Site to site replication software for virtual machines
Zip Tap	Zip tap

SCHEDULE 6

RIGHTS OF DATA SUBJECTS

1. *Data Subjects* have the following rights with regard to the *Personal Data* we hold about them, namely the right:

   (a) where Schedule 2 indicates TWM is relying on *Consent* to *Process* a *Data Subject's Personal Data*, to withdraw *Consent* at any time. However, this will not affect the lawfulness of any *Processing* carried out before the *Data Subject* withdraws their *Consent* or any *Processing* TWM carries out where we are not reliant on the *Data Subject's Consent*;

   (b) to receive certain information about the *Data Controller's Processing* activities;

   (c) to request access to the *Personal Data* that TWM holds about the *Data Subject* in order to check that it is accurate and complete and that we are *Processing* it lawfully;

   (d) to object to our use of the *Data Subject's Personal Data* for marketing purposes;

   (e) to ask us to delete or remove any of the *Data Subject's Personal Data* held by us where:

   - there is no good reason for us to continue to *Process* it;
   - the *Data Subject* has successfully exercised their right to object to *Processing* (see below);
   - TWM may have *Processed* a *Data Subject's Personal Data* unlawfully or where we are required to erase a *Data Subject's Personal Data* in order to comply with the law. Note, however, that we may not always be able to comply with a *Data Subject's* request for erasure for specific legal reasons which will be notified to the *Data Subject*, if applicable, at the time of their request

   (f) to ask us to correct any inaccurate or incomplete *Personal Data* held relating to the *Data Subject.* Note that we may need to verify the accuracy of the new *Personal Data* the *Data Subject* provides to us;

   (g) to ask us to suspend the *Processing* of a *Data Subject's Personal Data* where:

   - the *Data Subject* wants us to establish the *Personal Data's* accuracy;
   - our use of the *Personal Data* is unlawful but the *Data Subject* does not want us to erase it;
   - the *Data Subject* needs us to hold the data which we would not otherwise wish to hold for our own purposes, because the *Data Subject* needs it to establish, exercise or defend legal claims; or
   - the *Data Subject* has objected to our use of their *Personal Data* but we needs to verify whether we have overriding legitimate grounds to use it.

(h) to object to the *Processing* of the *Data Subject's Personal Data* where we are relying on a *Legitimate Interest* (or those of a third party) and there is something about the *Data Subject's* particular situation which they feel impacts unfairly on their fundamental rights and freedoms, though, in some cases, we may demonstrate that we have compelling legitimate grounds to *Process* that information which override such rights and freedoms;

(i) to request a copy of an agreement under which the *Data Subject's Personal Data* is transferred outside of the *EEA*;

(j) to object to decisions based solely on *Automated Processing*;

(k) to prevent *Processing* that is likely to cause damage or distress to the *Data Subject* or anyone else;

(l) to be notified of a *Personal Data* breach which is likely to result in high risk to their rights and freedoms;

(m) to make a complaint to the Information Commissioner's Office ("ICO"), the UK supervisory authority for data protection issues, at any time. We would, however, like the opportunity to deal with your concerns before you approach the ICO so please contact us in the first instance; and

(n) where the *Data Subject* has provided information to us in electronic form which we needed to perform a contract with the *Data Subject*, or where we are relying on the *Data Subject's Consent* for the right to *Process* the data, to ask for your *Personal Data* to be transferred to you or to a third party in a structured, commonly used, and machine-readable format.

2. If a *Data Subject* wishes to exercise any of the rights set out above, they should contact us by sending an email to our *DPO*, Matthew Truelove by email or by writing to him at TWM Solicitors LLP, 65 Woodbridge Road, Guildford, Surrey GU1 4RD.

3. *Data Subjects* will not normally need to pay a fee to access their *Personal Data* (or to exercise any of the other rights). However, we reserve the right to charge a reasonable fee if such a request is clearly unfounded, repetitive or excessively onerous. Alternatively, we have the right to decline to comply with such requests in these circumstances.

4. We may need to request specific information from a *Data Subject* to help us confirm their identity and ensure the *Data Subject's* right to access their *Personal Data* (or to exercise any of their other rights). This is a security measure to ensure that *Personal Data* is not disclosed to any person who has no right to receive it. We may also contact the *Data Subject* to ask them for further information in relation to their request in order to assist us to respond appropriately.

5. We endeavour to respond to all such legitimate requests within one month. Occasionally it may take us longer than a month if the request is particularly complex or the *Data Subject* has made a number of requests. In this case, we will notify the *Data Subject* and keep them updated.

SCHEDULE 7

JOB APPLICANT PRIVACY NOTICE

1. What is the purpose of this document?

TWM Solicitors LLP and TWM Trust Corporation Ltd (jointly referred to herein as "TWM" and "We") is a *Data Controller* and responsible for deciding how we hold and use *Personal Data* about you. You are being sent a copy of this privacy notice because you are applying for work with us (whether as an employee, worker or contractor). It tells you how and why your Personal Data will be used, namely for the purposes of the recruitment exercise, and how long it will usually be retained for. It provides you with certain information that must be provided under the General Data Protection Regulation ((EU) 2016/679) (GDPR).

2. Definitions of terms in italics in this Notice

***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.

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, signifies agreement to the *Processing* of *Personal Data* relating to them.

Data Subject: a living, identified or identifiable individual about whom we hold *Personal Data*. *Data Subject*s may be nationals or residents of any country and may have legal rights regarding their *Personal Data*.

***Data Protection Officer* (DPO)**: the person required to be appointed in specific circumstances under the *GDPR*.

Legitimate Interest: the interest of the firm in conducting and managing its business to enable it to give clients the best service and the best and most secure experience. We make sure we consider and balance any potential impact on data subjects (both positive and negative) and their rights before we *Process* their personal data for our *Legitimate Interest*s. We do not use their personal data for activities where our interests are overridden by the impact on them (unless we have their *Consent* or are otherwise required or permitted to by law).

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 *Sensitive 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.

Process or Processing: 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.

Sensitive Personal Data **(now called *Special Categories of Data* in the *GDPR*)**: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual orientation, biometric or genetic data, and *Personal Data* relating to criminal offences and convictions.

3. Data protection principles

TWM complies with data protection law and principles, which means that your data will be:

- Used lawfully, fairly and in a transparent way.
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
- Relevant to the purposes we have told you about and limited only to those purposes.
- Accurate and kept up to date.
- Kept only as long as necessary for the purposes we have told you about.
- Kept securely.

4. Why we *Process* your *Personal Data*

We need to *Process* data to take steps at your request prior to entering into a contract with you. We also need to *Process* your *Personal Data* to enter into a contract with you.

In some cases, we need to *Process Personal Data* to ensure that it complies with our legal obligations. For example, we are required to check a successful applicant's eligibility to work in the UK before employment starts.

We have a *Legitimate Interest* in *Processing Personal Data* during the recruitment procedure and for keeping records of the *Process*. *Processing Personal Data* from job applicants allows us to manage the recruitment *Process*, assess and confirm a candidate's suitability for employment and decide to whom to offer a job. We may also need to *Process Personal Data* from job applicants to respond to and defend legal claims.

Where we rely on *Legitimate Interest*s as a reason for *Processing Personal Data*, we have considered whether or not those interests are overridden by the rights and freedoms of candidates and have concluded that they are not.

6. The kind of information we hold about you

In connection with your application for work with us, we will collect, store, and use the following categories of *Personal Data* about you:

(a) The information you have provided to us in your CV and covering letter.

(b) If applying for a training contract, the information you have provided on our application form, including name, title, address, telephone number, personal email address, gender, employment history, qualifications including exam/degree/GDL/LPC details and results, positions of responsibility outside of employment, languages, charitable and pro bono endeavours, achievements, travel, other extra curricular activities, eligibility for employment in the UK, dates unavailable for interview and how you heard about TWM.

(c) Any information you provide to us during an interview or prior to interview.

(d) Test results, copies of relevant qualification certificates, your current practising certificate, your training record and a copy of your passport or other identification concerning your entitlement to work in the UK.

(e) Information about your current level of remuneration, including benefit entitlements.

(f) Information sought upon position being offered to you:

- address
- telephone number
- and start date.

(g) Information sought after the job offer has been accepted but prior to commencing employment**:**

- Criminal convictions and offences
- References
- Next of kin/emergency contact details
- Biography/profile for our intranet and a photograph
- Information for payroll purposes in the form of an HMRC Starter Checklist and/or P45 and a New Starter Form, including details such as bank account information, date of birth, NI number, student loan, PAYE number, tax code, earnings for the tax year, the amount you paid in tax in the tax year, and the date you finished working for your former employer.
- Whether or not you have a disability for which TWM needs to make reasonable adjustments during the recruitment *Process*.
- Equal opportunities monitoring information including socio economic background, caring responsibilities and "special category" information as mentioned below.

(h) We may also collect, store and use the following *Special Categories of Sensitive Personal Data:*

- Information about your race or ethnicity, religion or belief, sexual orientation. Information about your health including any medical/health conditions,

health and sickness records (information sought only after a job offer has been accepted but prior to commencing employment).

We will only collect and use *Sensitive Personal Data* (for example about your race or ethnicity, religious beliefs, sexual orientation and political opinions, trade union membership, health and sickness records) when we are entitled to do so, for example when that is with your explicit consent, or if you have manifestly made that information public, or if that is necessary for prescribed purposes laid down by law.

7. How is your *Personal Data* collected?

We collect *Personal Data* about candidates from the following sources:

- You, the candidate.
- Recruitment agencies.
- Job sites
- We collect the following categories of data from Recruitment Agencies and/or jobsites:

  (a) Name, title and gender;

  (b) Your current location;

  (c) Current level of remuneration details including benefit entitlements;

  (d) Value of a following if appropriate and targets achieved;

  (e) Employment history;

  (f) Qualifications including exam/degree/GDL/LPC details and results;

  (g) Positions of responsibility outside of employment, languages, charitable and pro bono endeavours, achievements, travel, extra curricular activities (if applicable);

  (h) Whether you have a disability for which the organisation needs to make reasonable adjustments;

  (i) Eligibility for employment in the UK; and

  (j) Dates available for interview.

- The Solicitors Regulation Authority for background check purposes, from which we collect the following categories of data:

  Fee earners: confirmation that you hold a current practising certificate, that you have been admitted to the roll of solicitors of England and Wales and that there are no findings or orders that have been made by the SRA and/or the Solicitors Disciplinary Tribunal against you.

Support Personnel: confirmation that you are not subject to any restrictions from the SRA limiting or prohibiting your right to work in a legal practice

- The Disclosure and Barring Service in respect of criminal convictions (collected via Atlantic Data software only after a job offer has been accepted but prior to commencing employment).

- Your named referees, from whom we seek to collect the following categories of data:

  (a) Dates employed;

  (b) Position(s) held;

  (c) Professional and interpersonal skills including strengths and weaknesses;

  (d) Number of days absent through sickness in the last year;

  (e) Whether there was any form of formal performance management/disciplinary action within the last 12 months;

  (f) Whether the referee would re-employ; and

  (g) Any additional information the referee may wish to supply.

8. How we will use *Personal Data* about you

We will use the *Personal Data* we collect about you to:

- Assess your skills, qualifications, and suitability for the work or role;

- Carry out background and reference checks, where applicable;

- Communicate with you about the recruitment *Process*;

- Keep records related to our hiring *Processes*; and

- Comply with legal or regulatory requirements.

It is in our *Legitimate Interest*s to decide whether to appoint you to a role or provide certain work.

We also need to *Process* your *Personal Data* to decide whether to enter into a contract of employment or a contract for services with you.

Having received your CV and covering letter (and, in some cases, your application form), along with any additional information provided by a recruitment agency (see above) or provided directly to us by you (such as location and remuneration package), we will then review that information to decide whether you meet the basic requirements to be shortlisted for the role. If you do, we will decide whether your application is strong enough to invite you for an interview. If so, we will use the information you provide to us at the interview, and test results if applicable, to decide whether to offer you the role or work. If we decide to offer you

the role or work, we will then take up references and carry out SRA and Law Society checks before confirming your appointment.

9. If you fail to provide *Personal Data*

If you fail to provide *Personal Data* when requested, which is necessary for us to consider your application (such as evidence of qualifications or work history), we will not be able to progress your application further.

10. How we use particularly Sensitive Personal Data

We will use your particularly *Sensitive Personal Data* in the following ways:

- We will use information about your disability status to consider whether we need to provide appropriate adjustments during the recruitment *Process*, for example whether adjustments need to be made during a test or interview.

- We will use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual orientation to ensure meaningful equal opportunity monitoring and reporting.

11. Information about criminal convictions

Having regard to the nature of the firm's business and because it is in the *Legitimate Interest*s of the firm and our clients that we do so, we will carry out a criminal records check, as detailed above, in relation to all successful job applicants prior to them commencing work at our offices.

We have in place a Data Privacy and Information Management Policy (available on our website) which details the safeguards we have in place in order to protect the privacy and legal rights of the subject of such criminal records checks.

12. *Automated Processing* / decision-making

You will not be subject to decisions that will have a significant impact on you based solely on *Automated Processing* decision-making.

13. Data sharing

We will share your *Personal Data* internally for the purposes of *Processing* your application. This includes members of the HR team, interviewers involved in the recruitment *Process*, managers in the business area with a vacancy and IT Personnel if access to the data is necessary for the performance of their roles. Prior to commencing employment your profile for our intranet and a photograph will be supplied to our Marketing team.

We will only share your *Personal Data* to third parties prior to commencement of employment as follows:

- Recruitment agencies when obtaining further information about you prior to and during the interview process, providing feedback following interview, offering you the role, dealing with issues prior to commencing employment and during any rebate periods;

- Atlantic Data to check criminal convictions (although this is information is usually entered onto the software directly by you);

- The Solicitors Regulation Authority and the Law Society as detailed above; and

- Your named referees

All of TWM's third party service providers are required to take appropriate security measures to protect your *Personal Data* in line with our policies and data protection legislation. We do not allow our third party service providers to use your personal data for their own purposes. We only permit them to *Process* your *Personal Data* for specified purposes and in accordance with our instructions.

14. Data security

We have put in place appropriate security measures to prevent your *Personal Data* from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your *Personal Data* to those employees, agents, contractors and other third parties who have a business need to know. They will only *Process* your *Personal Data* on our instructions and they are subject to a duty of confidentiality. Details of these measures may be obtained from the HR Manager, Kathy Betts (contact details below).

Candidate *Personal Data* will be stored in a range of different places, in hard copy files, on HR.Net and on other IT systems (including email).

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

15. Data retention

We will retain your *Personal Data* for a period of 6 months from receipt if it is an unsolicited job application (except for unsolicited agency CVs which are not retained) or 1 year from the date the vacancy is successfully filled if in response to a vacancy advertisement or briefing, and 18 months for shortlisted trainee applications. We retain your *Personal Data* for that period so that we can show, in the event of a legal claim, that we have not discriminated against candidates on prohibited grounds and that we have conducted the recruitment exercise in a fair and transparent way. After this period, we will securely destroy your *Personal Data* in accordance with our data retention policy.

If we wish to retain your *Personal Data* on file, on the basis that a further opportunity may arise in future and we may wish to consider you for that, we will write to you separately, seeking your explicit *Consent* to retain your *Personal Data* for a fixed period on that basis.

16. Rights of access, correction, erasure, and restriction

Under certain circumstances, by law you have the right to:

- Request access to your *Personal Data* (commonly known as a *Data Subject* Access Request). This enables you to receive a copy of the *Personal Data* we hold about you and to check that we are *Processing* it lawfully.

- Request correction of the *Personal Data* that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.

- Request erasure of your *Personal Data*. This enables you to ask us to delete or remove *Personal Data* where there is no good reason for us continuing to *Process* it. You also have the right to ask us to delete or remove your *Personal Data* where you have exercised your right to object to *Processing* (see below).

- Object to *Processing* of your *Personal Data* where we are relying on a *Legitimate Interest* (or those of a third party) and there is something about your particular situation which makes you want to object to *Processing* on this ground. You also have the right to object where we are *Processing* your *Personal Data* for direct marketing purposes.

- Request the restriction of *Processing* of your *Personal Data*. This enables you to ask us to suspend the *Processing* of *Personal Data* about you, for example if you want us to establish its accuracy or the reason for *Processing* it.

- Request the transfer of your *Personal Data* to another party.

If you want to review, verify, correct or request erasure of your *Personal Data*, object to the *Processing* of your *Personal Data*, or request that we transfer a copy of your *Personal Data* to another party, please contact the HR Manager, Kathy Betts, by email or by writing to her at TWM Solicitors LLP, 65 Woodbridge Road, Guildford, Surrey GU1 4RD.

17. Right to withdraw *Consent*

When you apply for a role, you provide *Consent* for us to *Process* your *Personal Data* for the purposes of the recruitment exercise. We do not ask for such *Consent* if we do not need it. You have the right to withdraw your *Consent* for *Processing* for that purpose at any time. To withdraw your *Consent*, please contact the HR Manager. Once we have received notification that you have withdrawn your *Consent*, we will no longer *Process* your application and, subject to our retention policy, we will dispose of your personal data securely.

18. Person with overall responsibility for data protection at TWM

The person with ultimate responsibility for this Privacy Notice is the firm's Managing Partner, Compliance Officer for Legal Practice (COLP) and *Data Protection Officer*, Matthew Truelove. He has overall responsibility for data protection, privacy and information management at TWM. If you have any questions about how we handle your *Personal Data*, please contact Matthew by email or by writing to him at TWM Solicitors LLP, 65 Woodbridge Road, Guildford, Surrey GU1 4RD.

Finally, you have the right to make a complaint at any time to the Information Commissioner's Office ("ICO"), the UK supervisory authority for data protection issues. TWM would, however, like the opportunity to deal with your concerns before you approach the ICO so please contact Matthew Truelove as above in the first instance.

Matthew Truelove
Managing Partner
September 2018