DATA PROTECTION POLICY

1 Introduction to data protection

During the course of its activities and to carry out its duties under the Solicitors Act 1974 the SDT (and SDTAL) collects, stores and processes personal data about its staff, contractors and other workers and Tribunal Members as well as Applicants, Respondents, Legal Representatives, contracted suppliers and people that it deals with. We will do this correctly and lawfully, and in accordance with data protection legislation, predominantly the retained UK version of the General Data Protection Regulation ((EU) 2016/679) ("UK GDPR"), and the Data Protection Act 2018 ("DPA 2018").

Everyone at the SDT and SDTAL is obliged to comply with this policy when processing personal data. Any breach of this policy may result in disciplinary action for employees and could lead to the termination of contract/engagement for those who are not employees.

2 Background to the UK GDPR and DPA 2018

The purpose of the UK GDPR and DPA 2018 is to protect the "rights and freedoms" of natural persons (i.e. living individuals) and to ensure that personal data is not processed without their knowledge, and that it is processed in line with lawful conditions.

The legislation applies to the processing of personal data by automated means (i.e. by computer) and to processing as part of a filing system (i.e. certain categories of paper records).

3 Definitions used by SDTAL (from the UK GDPR)

Personal data – any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special categories of personal data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. UK GDPR treats data relating to criminal offences/convictions separately; however for the purposes of this policy, we include this data within 'special categories of personal data'.

Data controller – the natural or legal person or body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data processor - a natural or legal person or body which processes personal data on behalf of the controller.

Data subject – any living individual who is the subject of personal data held by an organisation.

Processing – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Personal data breach – a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. There is an obligation on the controller to report personal data breaches to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject.

4 Policy statement

This policy applies to staff, contractors and other workers of Solicitors Disciplinary Administration Ltd (SDTAL). It does not form part of any employee's contract of employment and may be amended at any time. For simplicity, this policy refers to the obligations on SDTAL and its staff throughout but for the avoidance of doubt this includes the SDT and applies to contractors and other workers. Tribunal Members, whilst not employees of the SDT or SDTAL, are expected to adhere to the principles and requirements set out in this document.

For the sake of transparency, this policy is also published on our website for other third parties to see how we process personal data fairly, lawfully and transparently and in accordance with the UK GDPR and DPA 2018.

We recognise the importance of data protection in maintaining confidence in the SDT and SDTAL.

SDTAL's Management Team is committed to compliance with the UK GDPR and the DPA 2018 and the protection of the "rights and freedoms" of individuals whose information we collect and process.

Compliance with the UK GDPR and DPA 2018 is described by this policy and other relevant policies and procedures such as the Privacy Notices, Data Retention Policy, Personal Data Breach Management Policy and Procedure, IT and Communications Systems Policy and Procedure.

This policy applies to all of SDTAL's personal data processing functions, including those performed on the personal data of or received from employees, contractors and other workers of SDTAL and Applicants, Respondents, Legal Representatives, Tribunal Members, contracted suppliers and other people that the SDT and SDTAL deal with.

The Data Protection Co-Ordinator is responsible for reviewing the register of processing annually in the light of any changes to SDTAL's activities and to any additional requirements identified by means of data protection impact assessments. This register will be made available on request by the Information Commissioner's Office ("ICO").

Any breach of the UK GDPR or DPA 2018 or this policy will be dealt with under SDTAL's disciplinary policy and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities. Complying with Data Protection legislation is also an important requirement of the SDT's Code of Conduct for Members.

5 Responsibilities and roles under the UK GDPR and the DPA 2018

The SDT/SDTAL is a data controller under the UK GDPR in relation to a large of amount of personal data and may also be a data processor in relation to other personal data from other data controllers.

Compliance with the UK GDPR and the DPA 2018 is the responsibility of everyone at SDTAL – as everyone will process personal data, which can include merely accessing or receiving such data as part of their role.

SDTAL personnel must ensure that any personal data about them and supplied by them to SDTAL is accurate and up-to-date (including where appropriate relating to their dependents, next of kin, etc).

SDTAL's Management Team, Data Protection Co-Ordinator and those with managerial or supervisory roles throughout SDTAL are responsible for developing and encouraging good information handling practices within SDTAL.

The Data Protection Co-Ordinator is accountable to the CEO of SDTAL for the management of personal data and for ensuring that compliance with the UK GDPR and DPA 2018 and good practice can be demonstrated. This accountability includes development and implementation of DPA 2018 compliance as required by this policy.

The Data Protection Co-Ordinator has specific responsibilities in respect of procedures and is the first point of call for SDTAL personnel seeking clarification on any aspect of data protection compliance.

6 Data protection principles

All processing of personal data must be conducted in accordance with the data protection principles as set out in Article 5 of the UK GDPR.

SDTAL's policies and procedures are designed to ensure compliance with these principles, though it should be noted that there are exceptions which apply to these general and overarching values.

<u>Principle 1: Personal data must be processed lawfully, fairly and transparently</u>

Lawfully: SDTAL must identify a lawful basis before we can process personal data. This is often referred to as the "conditions for processing".
Fairly: in order for processing to be fair, SDTAL must make certain information available to the data subjects as required under the UK GDPR regardless of whether the personal data was obtained directly from the data subjects or from other sources.

Transparently: the UK GDPR includes comprehensive requirements for SDTAL to provide privacy information to data subjects. These are detailed and specific, placing an emphasis on making privacy notices understandable and accessible.

Please note that, in certain circumstances, it may not always be appropriate to alert every data subject about the processing activities that SDTAL or the SDT Tribunal Members undertake on behalf of SDTAL. Where disclosure of personal data is necessary for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings); necessary for the purpose of obtaining legal advice; necessary for the purpose of establishing, exercising or

defending legal rights, transparency is not always required where it would prevent SDTAL from making the disclosure.

Principle 2: Personal data can only be collected for specific, explicit and legitimate purposes

Data obtained for specified purposes by SDTAL must not be used for a purpose that differs from those formally notified to data subjects. If SDTAL wishes to use the personal data for a different purpose, it will notify the data subjects prior to the new processing taking place and will ensure that a lawful condition applies before undertaking the new processing activity.

Principle 3: Personal data must be adequate, relevant and limited to what is necessary for processing (aka "data minimisation")

SDTAL must not collect data that is not strictly necessary for the purpose for which it is obtained.

Principle 4: Personal data must be accurate and kept up to date with every effort to erase or rectify without delay

Data stored by SDTAL must be reviewed and updated as necessary. Whilst usually no data should be kept unless it is reasonable to assume that it is accurate, there are again exceptions, particularly where it is necessary to keep a record of data as it existed at a given point in time.

SDTAL reviews on at least an annual basis the retention dates of all the personal data processed and data which is no longer required to be held will be securely deleted/destroyed in line with the procedures are set out in section 10 of this Policy.

Principle 5: Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.

It follows from the commentary for Principle 4 that wherever possible and practicable, if personal data is retained by SDTAL beyond the processing date, access to it should be restricted (and it could also be minimised, encrypted or pseudonymised in order to protect the identity of the data subject in the event of a data breach).

The Data Protection Co-Ordinator must specifically approve any data retention that exceeds the retention periods defined in retention of records procedures, as set out in section 10 of this Policy.

Principle 6: Personal data must be processed in a manner that ensures the appropriate security

In determining appropriateness, the Data Protection Co-Ordinator will also consider the extent of possible damage or loss that might be caused to data subjects if a security breach occurs, the effect of any security breach on SDTAL itself, and any likely reputational damage including the possible loss of trust.

The additional "accountability" principle – the data controller must be able to demonstrate compliance with the other Principles

The UK GDPR includes provisions that promote accountability and governance, including Article 5(2) which requires SDTAL to demonstrate compliance with the principles above.

SDTAL demonstrates compliance by implementing policies, adhering to procedures and best practice, and implementing appropriate technical and organisational measures (including data

protection by design and by default, breach notification procedures and incident response plans etc).

7 Data subjects' rights

Data subjects may be able to exercise a number of rights in relation to the processing of their data by SDTAL. These include the right to:

- make access requests: regarding the nature of information held and to whom it has been disclosed (Subject Access Requests).
- correction and deletion: rectify, block, erase (including the right to be forgotten) or destroy inaccurate data.
- prevent processing: likely to cause damage or distress, or for the purposes of direct marketing.
- complain to SDTAL: relating to the processing of their personal data or the handling of requests.
- claim compensation: if they suffer damage by any contravention of the UK GDPR or the DPA 2018.
- involve the ICO: to assess whether any provision of the UK GDPR or the DPA 2018 has been contravened.
- portability: to have personal data transmitted in an electronic format to another controller.

However, it should be noted that a data subject's right to be notified that SDTAL even has their data in the first place, or their right to access, correction, erasure, etc, may be removed or curtailed where SDTAL can show that it is necessary on the basis of compelling legitimate grounds, for compliance with a legal obligation, for the performance of a task carried out for reasons of substantial public interest or the establishment, or the exercise or defence of legal claims.

The identity of an individual requesting data under any of the rights listed above must be verified. All staff must immediately forward any data subject request received to the Data Protection Co-Ordinator.

8 Lawful basis for processing

The UK GDPR and DPA 2018 are not intended to prevent the reasonable day-to-day processing of personal data, but to ensure that it is done lawfully, fairly and transparently.

For personal data to be processed lawfully, such data must be processed on the basis of one of the lawful grounds set out in the UK GDPR. These include (i) the data subject's consent to the processing, (ii) that the processing is necessary for the performance of a contract with the data subject, (iii) for the compliance with a legal obligation to which the data controller is subject, (iv) for the legitimate interests of the data controller or a third party or (v) for processing necessary for a public task set out in law. In connection with special category personal data, i.e. sensitive personal data, an additional condition must also be met.

<u>Consent</u>

For consent to be valid, it must have been explicitly and freely given, and a specific, informed and unambiguous indication of the data subject's wishes. As the data controller, if consent is being relied upon, SDTAL must be able to demonstrate that consent was obtained for the processing operation, and that the data subject can then withdraw their consent at any time.

In practice, except in very limited circumstances, SDTAL is unlikely to rely on consent as a lawful basis for processing any personal data.

For special categories of personal data, explicit written consent of data subjects must be obtained unless an alternative basis for processing exists, such as processing may be "necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement".

Necessary for the performance of a contract with the data subject

This is the lawful basis on which SDTAL will often rely in relation to processing the personal data of its staff, contractors and other workers as well as Tribunal Members and contracted suppliers.

Compliance with a legal obligation to which the data controller is subject

This lawful basis can be relied upon when SDTAL processes personal data in relation to records relating to, for instance, PAYE, pensions and tax, by virtue of its legal obligations to comply with the common law, statute and regulations.

Legitimate interests of the data controller or a third party

SDTAL will most commonly rely on this as a lawful basis for processing personal data on grounds that it is in the legitimate interests of SDTAL and/or third parties (to include personnel, clients, suppliers etc) to do so. Such interests will differ according to the specific circumstances but, broadly, much of the processing undertaken by SDTAL is likely to be in the legitimate interest of SDTAL carrying out its function / purpose in the most effective way.

When relying on legitimate interests as a lawful basis for processing personal data, SDTAL will always consider the interests and rights of the data subject.

Necessary for the discharge of a public task

This lawful basis can be relied upon when SDTAL processes personal data in the exercise of official authority discharging functions and powers set out in law. The processing must be *necessary* to the discharge of the function or power. SDTAL carries out specific processing required in order to discharge its obligations under the Solicitors Act 1974. This will cover the processing of personal data of Applicants, Respondents and Legal Representatives.

Further information on the lawful bases for processing personal data can be found in the SDTAL Privacy Notices.

9 Security of data

Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

SDTAL personnel are responsible for ensuring that any personal data that SDTAL processes and for which we are responsible as part of our roles, is kept securely and is not disclosed to any third party unless that third party has been specifically authorised by SDTAL to receive that information and has entered into a contract recognising their role as a data processor (see section 16 of this Policy).

The IT and Communications Systems Policy and Procedure sets out detailed policies and procedures on Information Security, though what follows are the golden rules when it comes to protecting personal data.

- The only people able to access data covered by this policy should be those who need it for their work.

- Data should not be shared informally. If a SDTAL member of staff requires access to confidential information for a specific purpose, they can request access to it from their line manager or the Data Protection Co-Ordinator.

- SDTAL will provide training to all personnel to help them understand their responsibilities when handling personal data.

- SDTAL personnel should keep all data secure, by taking sensible precautions and following the guidelines in this policy and the IT and Communications System Policy and Procedure.

- In particular, strong passwords must be used and they must never be shared. They must not be stored centrally, in personal files or on paper.

- Personal data must not be disclosed to unauthorised people, either within SDTAL or externally.

- Data must be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and securely disposed of.

- SDTAL Personnel must request help from the Data Protection Co-Ordinator if they are unsure about any aspect of data protection.

10 Retention and disposal of personal data

SDTAL shall not keep personal data in a form that permits identification of data subjects longer than SDTAL has determined is necessary, in relation to the purposes for which the data was originally collected or for other purposes in accordance with law or best practice.

The retention period for different categories of personal data is set out in the Data Retention Policy along with the criteria used to determine this period, including any legal or statutory obligations SDTAL has to retain the data.

Personal data must be disposed of securely in accordance with the sixth principle of the UK GDPR – which requires that such data is processed in an appropriate manner to maintain security, thereby protecting the rights and freedoms of data subjects.

SDT Members will ensure that they protect the personal data supplied to them in relation to specific cases with which they are involved and will securely destroy all such personal data (or arrange for the relevant clerk to do so) when the case is concluded in accordance with the Data Retention Policy. Tribunal Members in any doubt about their obligations or the requirements of Data Protection legislation generally should contact the Data Protection Co-Ordinator.

11 Data transfers outside the UK and EEA

The UK GDPR restricts data transfers to countries outside the UK to ensure that the level of data protection afforded to individuals by the UK GDPR is not undermined. Personal data originating in one country is transferred across borders when it is transmitted, sent, viewed or accessed in or to a different country.

The UK recognises countries within the European Economic Area ("EEA") as providing an adequate level of protection. The default position under the UK GDPR is that all exports of data to non-EEA countries or to countries that do not have a current 'adequacy agreement' with the UK are unlawful. Providing a third party outside the EEA with access to personal data or accessing such data from outside the EEA yourself will amount to 'transferring' or 'exporting' such data.

We do not envisage transferring personal data outside the EEA (other than in very rare circumstances, in which case the derogations will normally be relied upon, or some other lawful basis for transferring the personal data). If circumstances required that we transfer personal data outside the EEA, we will notify the Data Protection Co-Ordinator and seek guidance in advance. This is most likely to apply if you are considering using new software applications to process personal data.

12 Accountability

Data Protection Impact Assessments ("DPIAs")

DPIAs will be carried out where required in relation to the processing of personal data by SDTAL, and in relation to processing undertaken by third parties on behalf of SDTAL. This is where a type of processing, in particular using new technologies and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of individuals.

Data Protection Impact Assessments shall be overseen by the Data Protection Co-Ordinator and shall address the following:

1. the type(s) of personal data that will be collected, held, and processed;
2. the purpose(s) for which personal data is to be used;
3. SDTAL's objectives;
4. how personal data is to be used;
5. the parties (internal and/or external) who are to be consulted;
6. the necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;
7. risks posed to data subjects;
8. risks posed both within and to SDTAL and
9. proposed measures to minimise and handle identified risks.

Where, as a result of a DPIA it is clear that SDTAL is about to commence processing of personal data that could cause damage and/or distress to the data subjects, the decision as to whether or not SDTAL may proceed must be escalated for review to the Data Protection Co-Ordinator. If there are concerns, the Data Protection Co-Ordinator may need to escalate the matter to the ICO. Completed Data Protection Impact Assessments will be stored in a secure, central location to support any future audit or query.

Record-Keeping

SDTAL will keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

- the name and details of SDTAL, its Data Protection Co-Ordinator, and any applicable third-party data transfers (including data processors and other data controllers with whom personal data is shared);
- the purposes for which SDTAL collects, holds, and processes personal data;
- SDTAL's legal basis or bases (including, but not limited to, consent, the mechanism(s) for obtaining such consent, and records of such consent) for collecting, holding, and processing personal data;
- details of the categories of personal data collected, held, and processed by SDTAL and the categories of data subject to which that personal data relates;
- details of any transfers of personal data to non-UK countries including all mechanisms and security safeguards;
- details of how long personal data will be retained by SDTAL (please refer to SDTAL's Data Retention Policy);
- details of personal data storage, including location(s);
- detailed descriptions of all technical and organisational measures taken by SDTAL to ensure the security of personal data.

SDTAL's data protection compliance will be regularly reviewed and evaluated by means of Data Protection Audits (internal or external).

13 Personnel responsibilities and training

As noted, all personnel at SDTAL with day-to-day responsibilities involving personal data and processing operations, and those with permanent/regular access to personal data, must demonstrate compliance with the UK GDPR and the DPA 2018. The Data Protection Co-Ordinator may also assign specific data protection responsibilities, including in connection with training and awareness, to personnel as part of SDTAL's policies and procedures on personal data management and the accountability principle. For example, responsibilities in relation to the secure storage of electronically stored data and use of IT systems.

The Data Protection Co-Ordinator shall demonstrate and communicate to everyone at SDTAL the importance of data protection and information security in their role and ensure that they understand how and why personal data is processed in accordance with SDTAL's policies and procedures.

The Data Protection Co-Ordinator is responsible for organising relevant training for all responsible individuals and personnel generally, and for maintaining records of the attendance of staff at relevant training at appropriate intervals.

All staff and Tribunal Members are required to undergo data protection and information security training appropriate to their role, including mandatory refresher training from time to time, and to ensure they are aware of their responsibilities and obligations with regard to data protection.

14 Data breach notifications

Any information security breaches, near-misses, risks, weaknesses and events must be reported to the Data Protection Co-Ordinator, immediately after they are seen or experienced. Such issues could potentially range from major systems failures involving loss of services on the one hand (e.g. caused by external threats) to more minor breaches of information integrity on the other (e.g. an email sent to the wrong recipient). Please see the SDTAL Personal Data Breach Incident Management Policy for more details. It is important that you act promptly, as SDTAL only have 72 hours from becoming aware of the breach to assess the severity, and report to the ICO if required to do so.

15 Privacy Notices

SDTAL will always be transparent in its processing of personal data, subject to the derogations and exceptions noted in this Policy. SDTAL's Privacy Notices set out information to be provided to Data Subjects when SDTAL/the SDT collects information about them.

SDTAL will very rarely collect personal data from a data subject whilst relying on consent as the lawful basis for processing. Where this is the case, SDTAL will provide full and clear information on the processing purposes and in particular on the potential recipients.

When personal data has been obtained from a source other than the data subject, where required we will still take all reasonable steps to ensure and to demonstrate that the processing is fair and transparent, which includes explaining the categories of personal data received by SDTAL and the potential recipients.

Exceptions to the need to provide such information include:

- Where the data subject already has the information as it was provided to them by another party;
- If the provision of the above information proves impossible or would involve an excessive effort; or
- Where another exception applies which means that the provision of the privacy information is not required or not permissible.

We provide all employees with an Employee Privacy Notice to ensure that you understand what personal data we will process about you whilst you are employed by SDTAL. Please make the Data Protection Co-Ordinator aware if you have not received it or raise any questions you may have in relation to the notice.

16 Managing Data Processors

SDTAL will only select suppliers (to provide services to SDTAL) which can provide adequate technical, physical and organisational security in accordance with the UK GDPR/DPA 2018.

When the supplier meets the definition of SDTAL's data processor, including when data processing activities are not the primary reason for the contract, SDTAL as a data controller will ensure that adequate security arrangements are provided for in the contract with the external processor and that the requirements of Article 28 of the UK GDPR are met.

If the Data Protection Co-Ordinator considers it necessary because of the nature of the personal data to be processed or because of the particular circumstances of the processing, an audit of

the supplier's security arrangements must be conducted before entering into the contract. All revised data processing contracts allow SDTAL to conduct regular audits of the supplier's security arrangements during the period in which the supplier has access to the personal data.

SDTAL's processing contracts forbid suppliers from using further subcontractors without SDTAL's authorisation for the processing of personal data. Where we have permitted a supplier to subcontract the processing of personal data, the immediate supplier must prohibit the second-level contractor (or further down the chain) from subcontracting these processing operations without SDTAL's written authorisation. Contracts with second-level subcontractors will only be approved if they require the subcontractors to comply with at least the same security and other provisions as the primary subcontracting organisation (the initial supplier). Such contracts must specify that, when the contract is terminated, related personal data will either be destroyed or returned to SDTAL, and so on down the chain of sub-contracting.

Please ensure you consult the Data Protection Co-Ordinator in advance of agreeing any supplier contract terms, so that the centralised list of such suppliers is maintained.

17 Making a subject access or other request

If you reasonably believe that SDTAL processes your personal data, you can submit a subject access or other request relating to rights under the UK GDPR/Data Protection Act 2018.

The contact details of the SDT are:
2nd Floor
45 Ludgate Hill
London
EC4M 7JU

Our main office number is 0207 329 4808.
Email: enquiries@solicitorsdt.com

18 Complaints procedure

If you are dissatisfied with the Data Protection Co-Ordinator's response we would encourage you to discuss the decision with them. However, if an informal discussion does not resolve your complaint, you may submit it in writing to the Chief Executive Officer/Clerk either by e-mail to complaints@solicitorsdt.com or by post to the following address:

The Chief Executive Officer/Clerk
2nd Floor
45 Ludgate Hill
London
EC4M 7JU

Our main office number is 0207 329 4808.

They will consider your complaint, and will confirm, reverse or amend the decision and advise you in writing of the outcome.

You also have the right to apply to the Information Commissioner for a decision as to whether the Tribunal has dealt with your request for information in accordance with the requirements of Data Protection Act legislation and the UK GDPR.

An application may be made to the Information Commissioner's Office by post to the following address:

Information Commissioner's Office
Casework and Advice Division Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF.

The Information Commissioner's telephone help line is **0303 123 1113** The ICO's website is www.ico.org.uk. You can access further information about making a complaint at https://ico.org.uk/make-a-complaint/.