adcocks

Residential Property | Leasehold Reform
Commercial Property | Private Client

DATA PROTECTION, CONFIDENTIALITY AND INFORMATION SECURITY POLICY AND GUIDE

1.1 Purpose

This policy sets out how Adcocks Solicitors Limited complies with the General Data Protection Regulation (GDPR), confidentiality issues, information security and the SRA's regulatory requirements including outcome 7.5 and chapter 4 of the SRA Code of Conduct 2011. Guidance is also provided for employee's of the practice in order to assist with meeting their obligations of handling personal data they collect and process.

1.2 Application

This policy applies to all managers and employees of Adcocks, including those undertaking work through a consultancy arrangement, in a volunteer capacity, on a temporary basis, or through an agency. The term 'employees' is used to refer to managers and employees.
All employees must familiarise themselves, and comply with this policy and related procedures. Failure to comply with this policy and the related procedures may result in disciplinary action because of the significant risks of fines, enforcement action, reputational consequences and disciplinary action.

1.3 Responsibilities

All employees are responsible for ensuring that all types of data are properly protected. Any issues or concerns about the Regulation must be raised with Mark H Adcock.

1.4 Relevant legislation

The following legislation must be complied with:

- General Data Protection Regulation (GDPR);
- Data Protection Act 1998 (DPA);
- Computer Misuse Act 1990;
- Regulation of Investigatory Powers Act 2000;
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699);
- Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426);
- SRA Code of Conduct 2011.

1.5 Principles

The importance of keeping clients' affairs confidential, protecting personal and sensitive personal data and keeping information secure is fundamental. This policy is designed to cover all these areas so that all employees are clear about their obligations and how to protect data and ensure confidential information is kept confidential.
The GDPR establishes a framework of rights and duties designed to protect personal data. The GDPR requires that personal data is processed in compliance with the GDPR and in accordance with the six principles:-

1. Lawfulness, Fairness and Transparency
2. Purpose Limitation
3. Data Minimisation
4. Accuracy
5. Storage Limitation
6. Integrity and Confidentiality

Lawfulness, Fairness & Transparency

Personal Data must be processed lawfully, fairly and in a transparent manner. The data subject must be in a position to learn of the existence of a processing operation. The data must be as accurate as possible. The data controller and/ or processor should consider the fairness of collecting and processing data. Processing data is permitted where one or more of the following legal grounds have been established:

(a) Consent
Data controllers must obtain oral or written consent for data to be processed.
Pre-ticked boxes do not provide valid consent
Consent must be obtained fairly and honestly
Consent must identify the data controller and the purpose of the processing.
The consent must be capable of withdrawal by the data subject, as easily as giving consent.

(b) Performance of a contract
GDPR provides a legal basis for processing that is necessary for the performance of a contract to which the data subject is a party, or where processing is necessary in order to take steps at the request of the data subject prior to entering into a contract. If the data controller chooses to outsource processing activities to a data processor, consent must be obtained from the data subject prior to this taking place.

(c) Compliance with a legal obligation
Processing may be necessary for compliance with a legal obligation to which the controller is subject. The legal basis must be clear and precise, and its application foreseeable in accordance with the case law of the Court of Justice of the European Union and the European Convention on Human Rights.

(d) Vital interests of the data subject
GDPR permits processing that is necessary to protect the vital interests of the data subject or another natural person. 'Vital Interests' are generally interpreted as a life-or-death situation, where processing may serve both individual and public interest purposes.

(e) Public interest
Processing is permitted where it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

(f) Legitimate interests of the data controller
Lawful justification for processing where the interests of the data subject, and their fundamental rights and freedoms are not overridden. Example of legitimate interest may be the sharing of personal data to maintain cyber-security, or prevent fraud.

Purpose Limitation

Personal data must be collected for specific, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

Data subjects must be made aware of the purposes for which personal data is to be processed.

Data subjects should be provided with the firm's privacy notice.

Data may be processed for a further purpose if that processing is compatible with the first purpose.

Data Minimisation

Personal data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Accuracy

Steps should be taken to ensure that data is accurate and up to date where necessary and deleted or corrected if inaccurate.

Storage Limitation

Personal Data for clients and potential clients will only be stored for as long as deemed necessary in connection with the retainer.

Integrity and Confidentiality

Personal data must be processed in a manner that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational methods.

There are specific obligations particularly in relation to an individual's right to access data held about him or her. Chapter 4 of the SRA Code of Conduct 2011 contains the requirements relating to the duty of confidentiality. While solicitors have a duty to keep clients' affairs confidential, they must also ensure that information belonging to employees, suppliers and third parties is kept confidential. Confidential information can only be released if the individual consents or if that duty is overridden by law, e.g. the money laundering legislation.

The firm will have appropriate security to prevent personal data from being accidentally or deliberately compromised. Employees are reminded that under the Computer Misuse Act 1990, there are three criminal offences:

s.1: Unauthorised access to computer material.
s.2: Unauthorised access with intent to commit or facilitate the commission of further offences.
s.3: Unauthorised modification of computer material.

Employees who are unsure as to whether they are able to access or modify material must contact Mark H Adcock for guidance. Any commission of or attempt to commit a criminal offence by an employee will be dealt with in accordance with the firm's disciplinary policy.

As the firm monitors and stores the electronic communications of fee earners and other employees for business/security reasons, the firm must comply with the relevant provisions of the Regulatory and Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699). Further information is contained in the office manual.

All employees must keep information about the clients and the firm secure at all times. If an employee is concerned that data or confidential information is at risk, he or she must immediately contact Mark H Adcock.

1.6 Data Protection

The firm must keep certain information on its clients, employees and suppliers to carry out its day-to-day operations, to meet its objectives and to comply with legal obligations. The Regulation applies to personal data and sensitive personal data but the firm must keep all client (and employee) information confidential and all information secure.

The firm is committed to ensuring personal data is dealt with in compliance with the Regulations. The aim of the Regulations is to protect the rights of individuals (data subjects) about whom the firm holds 'personal data'.

The firm is registered with the Information Commissioner's Office. The person in charge of Data Protection at the firm is Mark H Adcock, With Hedley J Adcock in deputy position.

'Personal Data' means data which relates to a living individual who can be identified from that data or from that data and other information which is in the possession of or likely to come into the possession of the firm. Examples are a person's name, address and date of birth but the definition also includes information which allows an individual to be identified, e.g. a unique reference number. The definition includes any expression of opinion about the individual and any indications of the intentions of the data controller or any other person in respect of the individual.

Personal data includes all data held electronically but also data held in a 'relevant filing system', i.e. non-automated records which are structured in a way which allows ready access to information about individuals.

All personal data must be processed in accordance with the eight data protection principles which require that data will:

- be obtained fairly and lawfully and not be processed unless certain conditions are met;
- be obtained for a specific and lawful purpose;
- be adequate, relevant but not excessive;
- be accurate and kept up to date;
- not be held longer than necessary;
- be processed in accordance with the rights of data subjects;
- be subject to appropriate security measures;
- not be transferred outside the European Economic Area (EEA).

The firm must process personal data in accordance with one of the conditions for processing (usually consent) and fairly and lawfully.

Clients are provided with the necessary information about how their data will be processed in the client care letter and/ or terms of business. If clients have any queries, employees must contact Mark Adcock, or Hedley Adcock for advice.

1.7 Sensitive Personal Data

The firm may process data about clients which will include sensitive personal data. The terms of business explain to clients how their data will be processed and seek explicit consent to the processing. If a client has a query about sensitive personal data, guidance should be sought from the firm.

All employees must ensure that they recognise sensitive personal data. All employees must ensure that, wherever the data is held, i.e. on computer or in a relevant filing system (or a paper file), it is properly protected and held securely.

Sensitive personal data is personal data about:

(a) racial or ethnic origin;
(b) political opinions;
(c) religious or other beliefs of a similar nature;
(d) trade union membership;
(e) physical or mental health or condition;
(f) sexual life;
(g) the commission or alleged commission of any offence;
(h) any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

All employees will be trained on data protection issues and must attend the data protection training so that they understand what is meant by personal data and sensitive personal data and what their obligations are.

1.8 Employees

The firm also processes data about prospective and current employees in accordance with the firm's HR policies and the employment legislation as follows:

- Information on applicants for posts, including references.
- Employee information – contact details, bank account number, payroll information, supervision and appraisal notes.

All employees must comply with the same obligations in relation to employee data as they do in relation to client data.

1.9 Duty of Confidentiality

The duty of confidentiality to clients is a fundamental duty and for solicitors and their employees. Outcome 4.1 of the SRA Code of Conduct 2011 requires that the affairs of clients are kept confidential unless disclosure is required or permitted by law or the client consents.

Employees must tell a client all the information relevant to that retainer of which he or she has personal knowledge under outcome 4.2. Where the duty of confidentiality to one client conflicts with the duty of disclosure to another client, the duty of confidentiality takes precedence under outcome 4.3. Employees must ensure that they comply with the firm's conflicts policy.

Employees must comply with outcome 4.4 and must not act for client A in a matter where A has an interest adverse to client B and B is a client for whom confidential information is held which is material to A in that matter. The only exception to that prohibition is where a legal practice is able to use an information barrier.

The firm has effective systems and controls which are set out in the policies and procedures to identify risks to client confidentiality and to mitigate those risks, as required by outcome 4.5. Employees must comply with the firm's policies and procedures.

Employees must ensure conversations about client matters, which take place outside a secure environment, e.g. in the reception area, the lift and outside the office (especially with mobile phone conversations in public places, including trains) cannot be overheard.

Employees must not name clients or inform or confirm to a third party that the firm acts for someone unless that client has expressly given consent. This extends to enquiries from law enforcement as to whether the firm is acting for a particular individual which must be dealt with in accordance with the policy on responding to requests from law enforcement.

Employees must not answer any questions from the press or even confirm that the firm is acting for a particular client. Employees cannot provide an address (but can offer to pass on a letter to a client) and must refer all enquiries to Mark H Adcock or another partner.

When in court, employees must ensure that they do not discuss the client's matter in the hearing of the press or third parties, including the other parties to the case unless it is in the course of carrying out the client's instructions.

All employees must be aware of their duties under this policy and keep clients' affairs confidential except in the following situations:

- the client consents or asks that confidential information be provided;
- confidential information has to be provided by law.

All employees must comply with this policy and related procedures, attend training provided, raise any queries with Mark H Adcock and report any breaches or allegations or suspicions of breaches of confidentiality to the Mark H Adcock.

While the above provisions relate to clients, employees must ensure that they also keep information about other employees, third parties and suppliers confidential, as required by the law of confidence. The provisions apply equally to other employees, third parties and suppliers.

1.10 Personal Conflicts

If employees have any personal knowledge of or any close connection to the client or others involved in any matter on which they are working, they must comply with the firm's conflicts policy.

1.11 Information Security

All files, laptops, smartphones and mobile phones must be kept with the employee at all times to minimise the risk of breaches of confidentiality and ensure that information is kept securely.

All electronic devices issued by the legal practice will be encrypted so that the risk of data loss is reduced. Employees must comply the firm's policy in relation to any confidential information which may be held on their personal devices.

Employees are not permitted to use USB sticks, or other mechanisms of transferring data, on electronic devices owned by the firm unless approval has been received from Mark H Adcock.

When out of the office, files/papers must not be carried in a way which shows information that can identify the client (e.g. Mrs McGregor, 43 Acacia Avenue, Divorce). Files/papers must not be left in unlocked cars, and in no circumstances in cars overnight. If it is unavoidable, e.g. due to another appointment or court hearing, files/papers [may/must] be kept in the boot of a locked car.

All waste/unwanted letters and documents (including drafts and unwanted photocopies) must be disposed of securely in the confidential waste bins provided.

Employees must not:

- install any software without authorisation;
- disclose their password to anyone else;
- use other people's log-in details;
- take equipment, data, information sources or software offsite unless they have written authority to do so;
- copy files from the network server into a personal directory without authority.

Employees must:

- log off when leaving their PC or workstation unattended;
- change their password, if it appears to have been found out/in accordance with the firm's policy;
- ensure that no member of the public has access to the computer system;
- always ensure laptops and mobile devices are secured in unattended offices;
- ensure data is transferred between laptops/mobile devices and the main system as soon as possible to preserve its integrity and in accordance with the firm's policy;
- keep master copies of important data on the network server and not on a PC's local C drive or USB sticks. Data will not be backed up unless it is on the network server and so it is at risk;
- ask for advice from Mark H Adcock, if it is necessary to store, transmit or handle large quantities of data, e.g. DVDs or images.

If there is any loss of data or risk of loss, employees must immediately contact Mark H Adcock who will advise what to do next.

1.12 Subject Access Requests (SARs)

The GDPR gives individuals the right to access personal data held about them on computer and in relevant filing systems. Any person wishing to exercise this right should apply in writing to Mark H Adcock. The terms of business provide details of how to make a SAR.

If a request is made quoting the GDPR or if an individual makes a subject access request, that must be referred to the Mark H Adcock immediately. Clients may also ask for details of information held about them without mentioning the word 'data' or the data protection legislation; all such requests must be forwarded immediately to Mark H Adcock as that request may still be a SAR.

There are strict timescales for compliance with a SAR and failure to comply can result in a significant fine. Employees must comply with the firm's procedure for dealing with SARs.

1.13 Accuracy of Data

Employees must ensure that data is as accurate as possible; if data is or appears to be inaccurate, misleading or not up to date, employees must take reasonable steps to amend/update the information as soon as possible. Data only needs to be kept up to date where necessary and employees should seek guidance if they are not sure whether the data needs to be updated. Clients have the right to prevent processing of their personal data in some circumstances and the right to correct, rectify, block or erase information regarded as wrong. Any concerns must be discussed with Mark H Adcock.

1.14 Data Subject Rights

The Data Subject's rights are set out in chapter 3 of the GDPR and are summarised as follows:

(a) The right to transparency Data Subjects should be informed of processing activities concerning their personal data and informed of the consequences of doing so, or not doing so. Data controllers should provide the prescribed transparency information at the point in time when personal data is collected from the data subject. Data subjects must be informed if their data is processed for additional purposes, beyond the original purpose of collection.
Data controllers must provide the following information in a concise, transparent, intelligible and easily accessible form, using clear and plain language:

- The identity and contact details of the controller
- The contact details of Mark H Adcock in charge of Data Protection at the firm.
- The purpose of processing the data and its legal basis.
- Where processing is based on the data controller's legitimate interests, the legitimate interests pursued by the data controller or a third party.
- Any recipients of the personal data
- Details of any transfers to third countries and means of safeguarding
- The period for which personal data will be stored or the criteria used for determining such storage period.
- The existence of the right for data subjects to request from the controller the following in relation to their personal data: (a) access; (b) rectification; (c) erasure; (d) restriction; and (e) portability.
- Where processing is based upon the data subject's consent, the data subject's right to withdraw his or her consent at any time, without affecting the lawfulness of the processing based upon such consent prior to its withdrawal;
- The right to complain to the supervisory authority.
- Whether the provision of personal data is a statutory or contractual requirement, or is necessary to enter into a contract, and whether the data subject is obliged to provide such personal data and the consequences of failure to do so
- Any existence of automated decision making and the logic behind such decision.
- Any further processing activities beyond the initial purpose

(**b) Data collected from sources other than the Data Subject** The Data subject must be informed if personal data is obtained other than directly from the Data Subject. They must be informed of the data within 1 month of it being obtained. If the information is to be used to communicate with the data subject, the transparency information must be provided at the time of the first communication with the data subject and also if it is disclosed to a new recipient.

(c) The right to information and access to personal data Data controllers must confirm if they are processing data about a data subject and, if so, that data subject has the right of access to the personal data. Data subjects should have easy access to the information when requested. Requests to access personal data should be dealt with, within one month from the date when the request was received. This period may be extended for complex requests.

(d) The right to rectification Data subjects have the right to rectify inaccurate personal data held about them. The controller must also inform any third parties with whom they have shared the data, if possible, and necessary to do so.

(e) The right to erasure Data Subjects have a right to be forgotten where their personal data is no longer necessary for the purposes for which it was collected. Reference to Article 17 of the DPA should be made in regards to the Data Controllers obligation to erase personal data from its records.

There are exemptions to the right of erasure. Adcocks considers that automatically erasing personal data from its records after having completed its contractual obligations with clients, would not be in the interest of the client. Storing this information would be necessary to meet the firm's obligations to comply with the rules set by the Solicitor's Regulation Authority on storing data and files. The data could also be necessary for the establishment, exercise and defence of legal claims. The firm receives continuous requests for information about historical files and the erasure of this information would not be in the best interest's of the contracted client.

(f) The right to restriction of processing Data Subjects have the right to restrict processing of their personal data in certain circumstances: If the Data Subject contests the accuracy of their data held, the processing is unlawful, the controller no longer requires the personal data for the purpose of its processing, but the data subject requires the data for establishing, exercising or defending a legal claim or if the Data Subject has exercised the right to object to processing pursuant to Article 21(1) of the DPA.

(g) The right to Data Portability Data subjects have the right to receive their information from the data controller and re-use it with other service providers. There are restrictions and elements of privacy attached to this right which should be considered if a request from a Data Subject is received.

(h) The right to object to processing- The GDPR grants data Subjects a right to object to certain types of processing in a number of specific circumstances. The Data Controller must respond to the request within one month, with a potential two-month extension for complex or numerous requests.

(i) Rights in relation to automated decision making- Individuals are have rights when they are subject to automated decisions i.e decisions made entirely by technological means. Exemptions exist to this right and should be considered if the practice uses such methods of decision making.

1.15 Retention and destruction of data

Personal data must be retained or disposed of securely in accordance with the firm's data retention and destruction policy.

1.16 Data Controllers/Processors

Personal data must not be disclosed to another party unless they are a data controller or a data processor (as defined by this policy), it is for the purposes of the case. The client must always be advised to whom the data will be disclosed and why.

Before sending data to a data controller or a data processor, the employee must ensure that proper contractual arrangements are in place to protect the data. Alternatively the employee must contact Mark H Adcock to determine whether there is already a contractual arrangement or what further steps need to be taken. The firm must ensure that the data controller or data processor is clear as to the basis on which they will hold the data, when they will return it, what the security arrangements are and what will happen if there is any data loss.

Mark H Adcock is responsible for ensuring that appropriate due diligence is undertaken and that the firm is registered with the ICO. He will record the details of the data controller or data processor on the data controller/data processor log. If an employee has any queries about the way in which a data controller or data processor is dealing with data, he or she must contact Mark H Adcock.

1.17 Data Protection Impact Assessments (DPIA)

The GDPR guide states that DPIA's are

'Data Protection Impact Assessments (also known as privacy impact assessments or PIA's) are a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. An effective DPIA will aloow organisations to identify and fix problems at an early stage, reducing the associated costs and damage to reputation, which might otherwise occur.'

The circumstances in which a DPIA must be completed are when:

(a) using new technologies
(b) the processing is likely to result in a high risk to the rights and freedoms of individuals

1.18 Redaction

GDPR does not materially affect the circumstances where it is necessary to redact personal data. Guidance in this respect should be sought from the ICO document' How to disclose information safely'. It relates to the disclosure of information which has been derived from personal data and requires further processing to ensure that individuals cannot be identified from that information. There are several occasions when the firm should consider removing personal data:

(a) When responding to a Subject Access Request
(b) When making information available under the Freedom of Information Act 2000 (FOIA)
(c) When responding to information requests under the FOIA and disclosing third party personal data would break one of the data protection principles,
(d) And when redacting information that is outside the scope of an FOIA request, is the most efficient way of releasing relevant information that should be disclosed.

Careful attention to the regulations set by the Solicitors Regulation Authority should also be made when dealing with a request for information. Also see definition of 'Redaction' in clause 1.23 of this policy.

Care must be taken to ensure effective redaction. There are examples provided by the ICO whereby a marker pen used for redaction has not completely obscured text or, for digital information, text has been 'hidden' by highlighting it in black, however, that can easily be reversed if information is sent out electronically rather than in hard copy. In terms of solution, a black marker may not effectively redact information, but using a proper redaction pen and then photocopying or scanning the document will. Similarly, although redacting on Adobe may be reversible, if you then print out the document and scan it, that is not reversible.

1.19 Privacy Notice

The firm must continue to state to individuals why we retain their data; how we process it; and any rights which apply. The firm's privacy notice is:

Under the General Data Protection Regulations (May 2018), Adcocks must state the lawful bases for processing personal data.

adcocks

Residential Property | Leasehold Reform
Commercial Property | Private Client

We rely upon the following reasons for processing personal data:

1. **Consent:** Oral or written consent will be obtained for processing data.
2. **Performance of a contract:** The data subject is party to a contract and it is necessary for the performance of that contract to process personal data.
3. **Compliance with a legal obligation:** Processing is necessary for the compliance with a legal obligation to which the controller is subject.
4. **Legitimate interests of the data controller:** Lawful justification for processing where the interests of the data subject, and their fundamental rights and freedoms are not overridden.

We may use your personal data for the purpose of client identity verification, the provision of any of our services, the administration of files and records and legal and regulatory compliance. Further details of the work you are instructing us to do will be set out in our client retainer letter, together with a copy of our terms of business. Information will be held in hard copy and electronic form.

Our work for you may require us to provide information to third parties such as expert witnesses and other professional advisers. Any third parties to whom we disclose information about you, will be under an obligation to keep your information secure and not to use it for any purpose other than that for which it was disclosed. We may also disclose your personal data to third parties from whom we are buying a business/ assets or to whom we are selling some or all of our business/ assets as part of any due diligence process. Your personal data may subsequently be transferred to such third parties.

The work that we conduct for our clients can sometimes be lengthy and often correspond with other work that we are instructed to undertake. Adcocks will therefore retain personal data in line with our retention and deletion policies, via hard copy filing and electronic filing, unless we are asked to do otherwise. We will only use personal data for the purposes outlined above.

Adcocks will process your personal data in accordance with the General Data Protection Regulations, which came into force in May 2018.

Any concerns about how we handle your personal data or if you have any concerns about the contents of this Privacy Notice, please contact Mark H Adcock: ma@adcocks.com

1.20 Breaches of Policy

Breaches of this policy may require disclosure to the SRA, which may result in disciplinary action, given the obligations under chapter 10 of the SRA Code of Conduct 2011. A report may also need to be made to the ICO under the firm's policy on reporting to the ICO.

1.21 Compliance and Corporate Governance

This policy is intended to set out how the firm will meet its obligations under GDPR. The firm has less than 250 employees and therefore we only need to document data processing which is not occasional. This would apply to Subject Access requests and FOI requests (Under the Freedom of Information Act).

1.22 Further Advice

If there are concerns regarding a client or a retainer and potential breaches of confidentiality, employees must contact Mark H Adcock immediately for advice.

1.23 Definitions

Personal data – data which relates to a living individual who can be identified from that data, or from that data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Data subject means a living individual who is the subject of personal data.

Data controller means a person (usually an organisation) who (alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data is, or is to be, processed. However, two or more persons (usually organisations) can be joint data controllers where they act together to decide the purpose and manner of any data processing. The term 'in common' applies where two or more persons share a pool of personal data that they process independently of each other.

Data processor – in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

Redaction- (from the National Archives) 'The separation of disclosure from non-disclosable information by blocking out individual words, sentences or paragraphs or the removal of whole pages or sections prior to the release of the document. In the paper environment some organisations will know redaction as extracts when whole pages are removed, or deletions where only a section of text is affected'.

1.24 Related Policies and Procedures

The following policies and procedures must be considered when complying with this policy:

- Disciplinary policy
- Subject access request procedure
- Responding to requests from third parties policy
- Reporting to the ICO policy
- Data retention and destruction procedure
- Ongoing monitoring procedure
- Social media policy
- Data loss policy
- Complaints policy
- Training procedure.

1.25 Glossary

COLP	compliance officer for legal practice
GDPR	General Data Protection Regulation
DPA	Data Protection Act 1998
ICO	Information Commissioner's Office
SAR	subject access request
SRA	Solicitors Regulation Authority

Date of effect/date of review

This policy shall come into effect on 25th May 2018 and will be reviewed annually.