THREE RAYMOND BUILDINGS DATA PROTECTION POLICY

Point of contact: data.protection@3rblaw.com

1. Introduction

1.1. The protection of personal data and respect for individual privacy is fundamental to the day-to-day operations of Chambers.

1.2. This policy aims to protect and promote the data protection rights of individuals and of Chambers, by informing members and everyone working for and with Chambers, of their data protection obligations and of Chambers procedures that must be followed in order to ensure compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 1998 (DPA), taken together 'UK data protection legislation'.

1.3. This policy applies to all members of chambers, pupils, clerks, staff, consultants and any third party to whom this policy has been communicated.

1.4. This policy covers all personal data and special categories of personal data, processed on computers or stored in manual (paper based) files.

1.5. This policy applies to all members of chambers acting on behalf of chambers, and members of staff.

2. Responsibility

2.1. The IT sub-committee of chambers shall be responsible for drafting and from time to time amending this policy and for its implementation, under the supervision of the Management Committee.

2.2. Chambers' Manager is responsible for monitoring Chambers' compliance with this policy and shall be the central point of contact for data protection issues (in particular, the handling of subject access requests pursuant to Article 15 UK GDPR).

2.3. Everyone in Chambers to whom this policy applies is responsible for ensuring that they comply with this policy. Failure to do so may result in disciplinary action.

2.4. Chambers shall cooperate, on request, with the Information Commissioner's Office in the performance of the latter's tasks.

3. UK data protection legislation

3.1. UK data protection legislation is designed to protect individuals and personal data which is held and processed about them by Chambers or other individuals.

3.2. UK data protection legislation uses some key terms to refer to individuals, those processing personal data about individuals and types of data covered by the UK GDPR. These key terms are:

Personal data Means any information relating to an identified and identifiable natural person ('data subject'). This includes for example information from which a person can be identified, directly or indirectly, by reference to an identifier i.e.

	name; ID number; location data; online identifiers etc. It also includes information that identified the physical, physiological, genetic, mental, economic, cultural or social identity of a person. For Chambers' purposes, members of chambers, pupils, barristers' clients and Chambers' staff are data subjects (other individual third parties concerning whom we hold personal data about are also likely to be data subjects).
Controller	Means the natural or legal person, public authority, agency or other body who alone or jointly with others, determines the purposes and means of processing the personal data. In effect, this means the controller is the individual, organisation or other body that decides how personal data will be collected and used. For Chambers' purposes, this Chambers is a data controller for certain categories of data such as personal data relating to its members, staff and other third parties with whom it has a direct relationship.
Processing	Means any operation which is performed on personal data 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. For Chambers' purposes, everything that we do with client information (and personal information of third parties) is 'processing' as defined by the UK GDPR. This processing will often be in the capacity as a Data Processor on behalf of a Barrister as a Data Controller.
Processor	Means any natural or legal person, public authority, agency or other body that carries out any processing of personal data on behalf of a controller. Chambers acts as a processor in relation to personal data that it processes on behalf of members of Chambers.
Special category personal data	Means personal data revealing: a) racial or ethnic origin; b) political opinions; c) religious or philosophical beliefs; d) trade-union membership; e) the processing of genetic data or biometric data for the purpose of uniquely identifying a natural person; f) data concerning health or data concerning a natural person's sex life or sexual orientation; (g) data concerning criminal convictions.

4. Data Protection Principles

4.1. UK data protection legislation is based around **seven** principles as set out in the UK GDPR, which are the starting point to ensuring compliance with UK data protection legislation. Everybody working in, for and with Chambers must adhere to these principles in performing their day-to-day duties. The principles require Chambers to ensure that all personal data and special category personal data are:

4.1.1. Processed lawfully, fairly and in a transparent manner in relation to the subject ('**lawfulness**, **fairness** and **transparency**').

4.1.2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('**purpose limitation**').

4.1.3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('**data minimisation**').

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

4.1.5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which personal data are processed ('**storage limitation**').

4.1.6. Processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage using appropriate technical or organisational measures ('**integrity and confidentiality**').

4.2. Additionally, Chambers must be able to demonstrate its compliance with the six principles set out above ('**accountability**').

5. Processing personal data and special category personal data

5.1. When processing data on its own behalf, Chambers will only do so:

5.1.1. with the consent of the data subject;
5.1.2. where the processing is necessary for the performance of a contract to which the data subject is a party (or in order to take steps at the request of the data subject prior to entering into the contract);
5.1.3. where the processing is necessary for compliance with its legal obligations; or
5.1.4. where the processing is necessary for the purposes of the legitimate interests pursued by Chambers or by a third party (namely the provision of legal or related services, management of conflicts, complaints, training, staff administration), except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

5.2. You must:

5.2.1. have legitimate grounds for collecting and using the personal data;
5.2.2. not use the data in ways that have unjustified adverse effects on the individuals concerned;
5.2.3. be transparent about how you intend to use the data, and give individuals appropriate privacy notices when collecting their personal data;
5.2.4. handle people's personal data only in ways they would reasonably expect; and
5.2.5. make sure you do not do anything unlawful with the data.

5.3. You must ensure that you are aware of the difference between personal data and special category personal data and ensure that both types of data are processed in accordance with UK data protection legislation .

5.4. When processing special category personal data, Chambers will only do so when:

5.4.1. it has explicit consent from the data subject;
5.4.2. the processing is at the instruction of a member of chambers who is the data controller of that personal data;
5.4.3. the processing is necessary for the purposes of carrying out Chambers' obligations in respect of employment and social security and social protection law;
5.4.4. the processing is necessary to protect the vital interests of the data subject or another person;
5.4.5. the processing relates to personal data that has already been made public by the data subject; or

5.4.6. the processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

5.5. If you have any concerns about processing personal data, please contact a member of the IT sub-committee, who will be happy to discuss matters with you.

6. Retention

6.1. Chambers will process personal data:

6.1.1. on its own behalf as a data controller, only for so long as is necessary to comply with its legal obligations or for the purposes of providing services to its members; and

6.1.2. on behalf of members of chambers as a data processor, only for so long as instructed by the member of chambers.

6.2. In light of the above, when acting as a data controller, Chambers will normally retain personal data until after the expiry of any relevant limitation period in relation to potential legal proceedings, for example:

6.2.1. Contracts of employment, general personnel records, payroll and wage records – seven years after employment ends.

6.2.2. Employee bank details – as soon as possible after final payment has been made.

6.2.3. Staff recruitment records – six months after notifying candidates of the outcome of the recruitment exercise.

6.2.4. Records relating to tenancy recruitment from pupillage will also be retained for 3 years in order to provide external references.

6.2.5. The date of the last provision of service or goods, the date of the last payment made or received or the date on which all outstanding payments are written off, whichever is the latest.

At this point any further retention will be reviewed and the information will be marked for deletion or marked for retention for a further period. The latter retention period is likely to occur only where the information is needed for legal proceedings, regulatory matters or active complaints. Deletion will be carried out as soon as reasonably practicable after the information is marked for deletion.

6.2.6. Equality and diversity data may be retained for up to six years in anonymised form for the purpose of research and statistics and complying with regulatory obligations in relation to the reporting of diversity data.

6.2.7. Names and contact details held for marketing purposes will be stored indefinitely or until Chambers becomes aware or is informed that the individual has ceased to be a client or potential client.

6.3. Personal data processed by Chambers either as data controller or data processor will be periodically reviewed in order to ensure compliance with 6.1 above.

6.4. Personal data which should no longer be retained shall be destroyed or permanently deleted in a secure manner.

7. Rights of data subjects

7.1. The UK GDPR gives rights to individuals in respect of the personal data that any organisations hold about them. These rights include:

7.1.1. The right to be provided with information about how their personal data is processed.

7.1.2. The right to access the personal data that is being processed about them and to obtain a copy.
7.1.3. The right to rectification of any inaccurate personal data.
7.1.4. The right to erasure of personal data held about them (in certain circumstances).
7.1.5. The right to restriction on the use of personal data held about them (in certain circumstances).
7.1.6. The right to data portability (the right to receive data processed by automated means and have it transferred to another data controller).
7.1.7. The right to object to the processing of their personal data.

7.2. Chambers will process personal data in accordance with the rights of data subjects. Everybody working for Chambers must be familiar with these rights and adhere to Chambers' procedures to uphold these rights.

7.3. If anybody receives a request from a data subject (a client or other third party concerning whom we hold personal data) to exercise any of these rights, the request must be referred to the Chambers' Manager, immediately or to a member of the IT sub-committee in the absence of the Chambers' Manager.

8. Security of personal data

8.1. Chambers shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of likelihood and severity of its processing to the rights and freedoms of data subjects.

8.2. Such measures will include:
8.2.1. secure storage of digital and manual personal data;
8.2.2. encryption of digitally stored personal data;
8.2.3. password protection to all devices capable of accessing personal data;

8.3.

9. Confidentiality and data sharing

9.1. Chambers must ensure that it only shares personal data with the following individuals or organisations when it is permitted or obliged to do so in accordance with the law:

9.1.1. courts and other tribunals to whom documents are presented;
9.1.2. lay and professional clients;
9.1.3. potential witnesses, in particular experts, and friends or family of the data subject;
9.1.4. solicitors, barristers, representatives, pupils, mini pupils and other legal representatives;
9.1.5. ombudsmen and regulatory authorities;
9.1.6. current, past or prospective employers;
9.1.7. education and examining bodies;
9.1.8. third party service suppliers; and
9.1.9. business associates, professional advisers and trade bodies.

9.2. Chambers contracts with members of chambers that when acting as a data processor on behalf of members it will:

9.2.1. process data only on instructions from member of chambers;
9.2.2. ensure that persons authorised to process the personal data have committed themselves (through compliance with this Policy and the Staff Handbook) to confidentiality;
9.2.3. take all measures required to ensure the security of its data processing;

9.2.4. not engage third party suppliers / providers to process personal data controlled by member of chambers without the written authorisation of the relevant member of chambers, save where the law provides otherwise (where such authorisation is in general form, Chambers shall inform members of chambers of any intended changes concerning the addition or replacement of other processors, thereby giving member of chambers the opportunity to object to such changes);

9.2.5. only use third party suppliers / providers pursuant to a written contract which provides sufficient guarantees that the third party will implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the UK GDPR and ensure the protection of the rights of data subjects;

9.2.6. assist members of chambers by appropriate technical and organisational measures, insofar as is possible, for the fulfilment of members of chambers obligations to respond to requests for exercising of data subjects' rights under Chapter III of the UK GDPR;

9.2.7. assist members of chambers to ensure their compliance with Articles 32 to 36 of the UK GDPR;

9.2.8. at the choice of the data controller, delete or return all personal data as soon as practicable after the data controller ceases to be a member of chambers; and

9.2.9. make available to members of chambers all information necessary to demonstrate compliance with Article 28 of the UK GDPR and allow for and contribute to audits, including inspections, conducted by members of chambers.

9.3. Where a Chambers engages another processor to carry out specific processing activities on behalf members of chambers, the same obligations as set out at 8.2 above shall be imposed on that other processor by way of a contract or other legal act. Where that other processor fails to fulfil its data protection obligations, Chambers shall remain fully liable to members of chambers for the performance of that other processor's obligations.

9.4. Chambers will only share special category personal data with the following categories of third party as permitted or required by law:

10. Record keeping

10.1. Chambers shall keep a record of:

10.1.1. the name and contact details of each member of chambers who is a data controller on whose behalf Chambers acts as a data processor;

10.1.2. the categories of processing carried out on behalf of each data controller (as identified in their individual data protection policies);

10.1.3. where applicable, any transfers of personal data to third countries or organisations; and

10.1.4. where possible, a general description of the technical and organisational security measures applied to the personal data.

10.2. Chambers shall keep a record of all periodic reviews of personal data it processes in accordance with 6.1 above.

10.3. Chambers shall keep a record of the destruction and/or deletion of personal data pursuant to 6.4 above.

10.4. Chambers shall keep a record of data breaches pursuant to 11.4 below.

11. Breaches

11.1. A data protection breach is defined as "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" and may include circumstances in which personal data is:

11.1.1. accessed without authority;

11.1.2. processed unlawfully;
11.1.3. lost;
11.1.4. destroyed; or
11.1.5. damaged.

11.2. Everybody working in, for and with Chambers has a duty to report any actual or suspected data protection breach without delay to the Senior Clerk and the Chambers' Manager (or in their absence, a member of the IT sub-committee).

11.3. Breaches will be reported to the Information Commissioner's Office (ICO) by the Head of Chambers (or in his/her absence, his/her designated deputy) without undue delay and, where feasible, not later than 72 hours after having become aware of the breach, unless Chambers is able to demonstrate that the personal data breach is unlikely to result in a risk to the rights and freedoms of data subjects.

11.4. Chambers' Manager will maintain a central record of the details of any data protection breaches, comprising of the facts relating to the personal data breach, its effects and the remedial action taken.

11.5. Although, as data controllers, Barristers are under no regulatory obligation to report a breach to Chambers and are responsible individually for compliance with the notification and reporting obligations of UK data protection legislation, nonetheless, Chambers recognises the role undertaken by Chambers as a Data Processor and acknowledges an obligation to support Data Controllers in those cases where it is appropriate to do so. In the case of a data breach for which a member of chambers is the relevant data controller, the member of chambers is expected to report the breach to the Senior Clerk and the Chambers' Manager. Chambers in its capacity as data processor will support any member of chambers reporting and managing data breaches.

12. Data Protection Impact Assessments (DPIAs)

12.1. DPIAs are required to identify data protection risks; assess the impact of these risks; and determine appropriate action to prevent or mitigate the impact of these risks, when introducing, or making significant changes to, systems or projects involving the processing of personal data.

12.2. When a DPIA is required to be conducted pursuant to Article 35 UK GDPR, it will be undertaken by the IT sub-Committee or designated members of staff.

13. Complaints

13.1. Complaints relating to breaches of UK data protection legislation and/ or complaints that an individual's personal data is not being processed in line with the data protection principles should be referred to the Chambers' Manager (or in his/her absence, a member of the IT sub-committee) without delay.

14. Penalties

14.1. It is important that everybody working for Chambers understands the implications for Chambers if we fail to meet our data protection obligations. Failure to comply could result in:

14.1.1. criminal and civil action;
14.1.2. fines and damages;
14.1.3. personal accountability and liability;
14.1.4. suspension/withdrawal of the right to process personal data by the ICO;
14.1.5. loss of confidence in the integrity of the business's systems and procedures; and/or
14.1.6. irreparable damage to the business's reputation.