SIX PUMP COURT

DATA PROTECTION, PRIVACY & INFORMATION SECURITY POLICY OF LUCY LUTTMAN

PARTICULARS

Policy approval date:	1 April 2026
Policy operation date:	1 April 2026
Next review date:	1 April 2028
Data Controller:	Lucy Luttman
Registration Number:	Z2690210
'Chambers' means:	Six Pump Court Chambers Chambers of Stephen Hockman KC and Mark Watson KC, Temple, London, EC4Y 7AR.

PART ONE – INTRODUCTION

1. Overview

As a self-employed barrister and an independent **Data Controller** under the UK GDPR and Data Protection Act 2018, I am legally responsible for ensuring that all personal data I process in my practice is collected, used, stored, shared, transferred and destroyed lawfully, fairly and securely.

This Policy sets out how I, as a member of Six Pump Court Chambers ("Chambers"), must meet:

- UK GDPR & Data Protection Act 2018
- BSB Handbook (Core Duty 6 and rC15.5)
- Bar Mutual insurance requirements
- Chambers' Data Protection, Privacy & Information Security Policy ("Chambers Policy")
- ICO guidance (as updated)
- Cybersecurity and cloud governance standards
- Mandatory breach reporting, document hold, and retention rules

I must comply with this Policy as a condition of my membership of Chambers and as part of my professional regulatory obligations.

This Policy is publicly available on Chambers' website under my name. Accordingly, it is constructively brought to the attention of all clients, potential clients, sources of instruction, other members of the Bar, staff, employees, regulatory bodies such as the BSB or ICO, third-party contractors and service providers, and any other person with whom I deal as a barrister.

The Schedules to this Policy include the following Agreements:

1) Joint Controllers Data Sharing Agreement (**Schedule 1**)
2) Data Controller and Data Processor Agreement (**Schedule 2**)

Where relevant and applicable, these are binding on any person, organisation or body with whom I engage respectively as a **Joint Data Controller** or as a **Data Processor**.

2. Relationship Between This Policy and Chambers' Policy

This Policy:

- Mirrors the structure and obligations of Chambers' Policy
- Sets out the specific requirements applicable to me as a Data Controller and, where relevant and applicable, Joint Data Controller and Data Processor
- Works in tandem with Chambers' Policy, which governs Chambers' ICT, systems, staff, clerks and support operations
- Where relevant and applicable, incorporates Chambers' ICT configuration, security controls and Modern Desktop environment

Where obligations differ:

- Chambers' Policy governs the systems environment
- This Policy governs my individual legal responsibilities as Data Controller

If in doubt, the stricter standard applies.

3. Scope

This Policy applies to:

- All personal data and special category data processed in my practice
- All electronic and physical information handled by me, pupils, mini-pupils, or third-party processors acting on my behalf
- All processing undertaken inside or outside Chambers
- All devices used for professional purposes
- Cloud services, email, messaging and storage
- Chambers' staff, including clerks, insofar as they process personal data on my behalf as my Processor

4. Professional and Regulatory Foundations

I must comply with:

- BSB Core Duty 6 – Keep client information confidential
- rC15.5 – Take reasonable steps to protect client confidentiality
- ICO requirements for Data Controllers
- Article 6 UK GDPR lawful bases
- Article 9(2)(f) condition for legal claims
- Article 10 for criminal offence data (with Schedule 1 DPA 2018 conditions)

- Bar Mutual insurance obligations, including in relation to retention of records

PART TWO – GENERAL POLICIES

1. Information Security Framework

Unless a written exemption is in place, by reason of an authorised BYOD (Bring-your-own-device) Agreement or otherwise, I must comply fully with Chambers' secure ICT environment, including:

- Microsoft 365
- OneDrive with Conditional Access
- Chambers' networks (London and Maidstone)
- Chambers' practice management system (Lex)
- Centralised identity, MFA, configuration and security controls

I must not disable, modify, circumvent or override these protections.

2. Modern Desktop & Device Management

2.1 Managed Devices (default)

I must use a **Managed Device** unless formally approved for **BYOD** (Bring-your-own-device). Managed devices include:

- Automated patching
- Anti-malware
- Secure configuration
- Device encryption
- Remote-wipe and containment
- Ability for Chambers' IT provider to monitor security posture

Chambers maintains a log of all my computers and devices used for storing or working on case files. The log is maintained and updated from time to time and records type, model and serial number of each device, together with the details and currency of any anti-virus, anti-spyware, encryption or other security software maintained on each machine.

2.2 Self-Managed Devices (BYOD)

Only permitted when:

- A signed BYOD Agreement is in place
- Mandatory security controls are applied
- The device is registered with Chambers
- My OS, software and configuration meet equivalent controls to Managed Devices

I must not use:

- Jailbroken or rooted devices
- Devices without full-disk encryption
- Out-of-date or unprotected systems

3. Physical Security of Papers and Devices

I must ensure:

- Papers are transported discreetly and stored securely
- No papers are left in cars overnight
- No case materials are viewed in public or semi-public spaces
- Screens are angled to prevent shoulder surfing
- Devices are locked when unattended

Hard copy materials must be:

- Returned to Chambers when not in use
- Locked away securely at home
- Shredded using confidential waste facilities and not in household waste

4. ICT, Cloud and Email Use

4.1 Email

- All professional work must be conducted through Chambers' email system.
- Auto-complete must be used with extreme caution.
- Sensitive attachments must be encrypted, with passwords sent separately.
- Large files should be shared using secure links, not unencrypted email attachments.

4.2 Cloud Services

Unless a written exemption is in place, by reason of an authorised BYOD (Bring-your-own-device) Agreement or otherwise, I must use Chambers-approved:

- Microsoft 365
- OneDrive
- SharePoint

Use of any alternative cloud provider requires:

- Provider assessment
- Confirmation of confidentiality, deletion, and security guarantees
- Verification of international transfer safeguards

4.3 Public Wi-Fi

I must not access confidential materials on public Wi-Fi unless:

- Using a VPN
- Device discoverability is disabled

5. Social Media and Public Commentary

I must adhere to the social media policy of Chambers as set out in Chambers' Data Protection, Privacy and Information Security Policy or as otherwise provided to me in the Chambers Handbook.

The following general rules apply:

- Maintain client confidentiality.
- Do not disclose case details not in the public domain without client consent.
- Protect Chambers' commercial information.
- Do not disclose internal strategies.
- Use Chambers' branding only in accordance with approved guidelines.
- Cite sources accurately and respect third-party IP.
- Do not post material that could reasonably be seen as defamatory, discriminatory or otherwise damaging to Chambers or individuals.

PART THREE – DATA PROTECTION AND THE UK GDPR

1. The Seven Data Protection Principles

I must comply with:

1. Lawfulness, fairness & transparency
2. Purpose limitation
3. Data minimisation
4. Accuracy
5. Storage limitation
6. Integrity & confidentiality
7. Accountability

Where necessary and applicable, I must demonstrate compliance through:

- Policies
- Logs
- Retention schedules
- DPIAs
- Documented Instructions to Chambers as Data Processor

2. Lawful Bases

2.1 Article 6 Bases

Common bases I rely on:

- **Legitimate interests** – operating a barrister's practice
- **Contract** – instructions from a client
- **Legal obligation** – BSB, court or statutory duties
- **Vital interests** – if life or safety requires data processing

2.2 Special Category Data – Article 9

The primary legal basis is:

- **Article 9(2)(f)** – legal claims

2.3 Criminal Offence Data – Article 10

Requires:

- A Schedule 1 DPA 2018 condition

- An Appropriate Policy Document (APD)
- Secure handling and restricted access

3. Rights of Individuals

I must handle:

- Access requests (SARs)
- Rectification
- Erasure (where applicable)
- Restriction
- Portability
- Objections
- Rights relating to automated decision-making

SARs must be answered within **one month**, extended only where legally permitted.

Where Chambers handles emails or papers as Data Processor, I must coordinate with Chambers' clerks promptly.

4. DPIAs

I must complete a DPIA before:

- Large-scale or sensitive processing
- New data flows
- High-risk cases (e.g., political opinions, criminal data, vulnerable clients)

Any new device should be a Managed Device (default) unless approved as a Self-Managed Device (BYOD) and subject to the necessary protections. Before introducing new equipment, I should assess the impact on data protection, privacy and information security.

5. International Transfers

I aim to avoid international transfers where possible. If personal data is transferred internationally, it is only where lawful safeguards are in place.

Where transfers are necessary, I will first use adequacy (e.g., the UK-US Data Bridge where the US recipient is DPF-listed and opted into the UK Extension). Otherwise, I will use IDTA/UK Addendum (as appropriate) plus a Transfer Risk Assessment (TRA) and adopt any extra measures needed.

Use of the UK-US Data Bridge (UK Extension): I may transfer personal data to a US organisation only if that recipient appears on the Data Privacy Framework (DPF) List and is opted-in to the UK Extension. Where the US recipient is not on the DPF List (or is ineligible to participate), I will rely on IDTA or the UK Addendum (as appropriate) plus a TRA and will implement any additional measures identified by the TRA.

A TRA may require:

- Encryption
- Access restrictions
- Logging
- Contractual enhancements

PART FOUR – MEMBER OBLIGATIONS

1. Secure Working

I must:

- Avoid working on papers in public
- Keep papers out of sight when travelling
- Avoid leaving anything in cars overnight
- Use locked rooms and cabinets at home

2. Encryption & Secure Devices

All devices must have:

- Full-disk encryption
- MFA
- Automatic lock after short inactivity
- Up-to-date OS and patching
- Chambers Modern Desktop compliance (unless subject to a BYOD exemption)
- Anti-malware and secure configuration

File-level encryption must be used for highly sensitive matters.

3. Data Minimisation

I must:

- Work with the minimum amount of data necessary
- Avoid retaining duplicate sets of papers
- Delete working copies as soon as possible
- Keep no personal data on local storage if cloud storage is available

4. Retention and Disposal

My retention periods follow Chambers' category-based Retention Schedule, reflecting purpose and legal obligations including guidance from my insurer the Bar Mutual Indemnity Fund. Data is not kept longer than necessary. Document hold suspension applies where litigation or regulatory action is anticipated.

I must:

- Follow the retention periods in **Schedule 3**
- Apply document hold immediately when litigation is anticipated

- Destroy physical data via secure shredding
- Securely wipe electronic data
- Ensure cloud providers confirm deletion

5. Breach Reporting

I must:

- Report immediately to Chambers (the Senior Clerk, Heads of Chambers)
- Avoid deleting or altering affected data
- Cooperate with containment, investigation and notification
- Notify Chambers if the breach relates to any processing done on Chambers systems

Further information is provided in **Schedule 5**.

PRIVACY NOTICE – MEMBER

Introduction

I will take all possible steps to protect your personal information. I am determined to do nothing that would infringe your rights or undermine your trust. This Privacy Notice describes the information I collect about you, how it is used and shared, and your rights regarding it.

This Privacy Notice applies to data subjects who have sent me their personal data (Article 13 UK GDPR) and to data subjects who have not sent me their personal data but where I have received that personal data via a third party (Article 14 UK GDPR).

Data Controller

I am registered with the ICO as a Data Controller for the personal data that I hold and process as a barrister.

My registered address is:

Six Pump Court Chambers
The Chambers of Stephen Hockman KC and Mark Watson KC
6 Pump Court
Temple
London EC4Y 7AR

My ICO registration number is:

[insert number]

Data Collection

All the information that I hold about you is provided to or gathered by me in the course of a

case and/or proceedings and/or for another reason connected to my practice as a barrister.

If you have instructed me via a solicitor, your solicitor and I are Joint Data Controllers and we will tell you why we need the information and how we will use it. If you have instructed me via direct access or have instructed me to represent you, I will be the applicable Data Controller and I will tell you why I need the information and how I will use it.

I collect and process both personal data and special categories of personal data as defined in the GDPR. This includes:

- Names
- Emails
- Phone numbers
- Addresses
- Payment or bank details
- Dates of birth
- Location details
- Financial information
- Medical Records
- Criminal Records

Lawful Basis for Processing

The UK GDPR requires all organisations that process personal data to have a Lawful Basis for doing so. The Lawful Bases identified in the UK GDPR include:

- Consent of the data subject
- Performance of a contract with the data subject or to take steps to enter into a contract
- Compliance with a legal obligation
- To protect the vital interests of a data subject or another person
- Performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

- The legitimate interests of the data controller, or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject

Examples of legitimate interests include:

- Where the data subject is a client or in the service of the controller
- Transmission within a group of undertakings for internal administrative purposes
- Processing necessary to ensure network and information security, including preventing unauthorised access
- Processing for direct marketing purposes, or to prevent fraud
- Reporting possible criminal acts or threats to public security

The Lawful Basis on which I will process your data is that of my legitimate interests and my legitimate interests are, variously as the case may be:

- That I need to process your personal data as you are my lay client and I cannot represent you without processing your personal data.
- That you are a potential client and I need to process your personal data to market to you or to engage with you with a view to you becoming my client.
- That you are part of an instructing body or professional client such as a firm of solicitors or instructing department, and I cannot be instructed by you without processing your personal data.
- That you are a member, employee, contractor, staff member, pupil or mini-pupil of Chambers, or a prospective member of any of those classes of person, and I need to process your personal data in order to facilitate that relationship.
- That you are an opponent on a case, an employee of the Courts or another tribunal, a witness, family member or friend or other contact of my client, a judge or other decision maker, a member of a regulatory body such as the BSB, a member of the Bar Council, or any other third party of any other description whose personal data I will process for any reason howsoever connected to my practice, and in each case I will need to process your personal data in order to operate as a barrister.

Special category data is processed under appropriate Article 9 conditions, most commonly Article 9(2)(f) (legal claims), or where required, explicit consent or other valid conditions. Where relevant, criminal offence data is processed in accordance with Article 10 and Schedule 1 DPA 2018.

Use of Personal Data

I use your information to:

- Provide legal advice and representation
- Assist in training pupils and mini-pupils
- Investigate and address your concerns
- Communicate with you about news, updates and events
- Investigate or address legal proceedings relating to your use of my services/products, or as otherwise allowed by applicable law
- Make statutory returns as required by HMRC, the BSB or any other body

I do not use automated decision-making[1] in the processing of your personal data.

Sharing Personal Data

I may share your personal data with:

- Instructing solicitors or departments
- Pupils or mini-pupils under my training or under the training of other members of Chambers
- Other members of my Chambers
- Opposing counsel
- My Chambers management and staff who provide administrative services such as clerks
- The Bar Standards Board or other regulatory body or legal advisors in the event of a

[1] The process of making decisions solely by technological means without any human intervention.

dispute or other legal matter

- Law enforcement officials, government authorities, or other third parties to meet my legal obligations
- Publicly by way of marketing or advertisement where your case has been published in a law report or otherwise
- Judicial appointment bodies or legal rankings services
- Service providers carrying out services for me, such as ICT or internet service providers

Transfers Outside the UK

I aim to avoid international transfers where possible. If personal data is transferred internationally, it is only where lawful safeguards are in place.

Where transfers are necessary, I will first use adequacy (e.g., the UK-US Data Bridge where the US recipient is DPF-listed and opted into the UK Extension). Otherwise, I will use IDTA/UK Addendum (as appropriate) plus a Transfer Risk Assessment (TRA) and adopt any extra measures needed.

Use of the UK-US Data Bridge (UK Extension): I may transfer personal data to a US organisation only if that recipient appears on the Data Privacy Framework (DPF) List and is opted-in to the UK Extension. Where the US recipient is not on the DPF List (or is ineligible to participate), I will rely on IDTA or the UK Addendum (as appropriate) plus a TRA and will implement any additional measures identified by the TRA.

A TRA may require:

- Encryption
- Access restrictions
- Logging
- Contractual enhancements

Retention

I retain your personal data while you remain a data subject whose data I have a legitimate interest in processing, unless you ask me to delete it. My approach to Retention and Disposal is set out in this Policy (see, Part Four and Schedule 3).

I will delete or anonymise your information at your request unless:

- There is an unresolved issue, such as claim or dispute
- I am legally required to, or
- There are overriding legitimate interests, including but not limited to fraud prevention and protecting customers' safety and security.

Your Rights and Complaints

The UK GDPR gives you specific rights around your personal data. For example, you have to be informed about the information I hold and what I use it for, you can ask for a copy of the personal information I hold about you, you can ask me to correct any inaccuracies with the personal data I hold, you can ask me to stop sending you direct mail, or emails, or in some circumstances ask me to stop processing your details. Finally, if I do something irregular or improper with your personal data you can seek compensation for any distress you are caused or loss you have incurred. You can find out more information from the ICO’s website and this is the organisation that you can complain to if you are unhappy with how I dealt with you.

Accessing and Correcting Personal Data

You may request access to, correction of, or a copy of your information by contacting me via Chambers.

Updates

I will occasionally update my Privacy Notice. When I make significant changes, I will publish the updated Notice on my website profile.

SCHEDULES

Schedule 1 – Joint Controllers' Data Sharing Agreement

This Agreement is effective as between me and any Data Controller instructing me to carry out regulated activities as a barrister.

This Agreement is deemed to be dated on the date instructions are received, or a contract for services is formed.

Introduction

1. The parties to this Agreement will work together to advise, provide expertise to or represent lay clients in legal proceedings. The exchange of information facilitates this partnership and should always adhere to legal requirements under the UK GDPR.

2. For the purposes of this Agreement the Parties jointly handle and process personal data and sensitive personal data as defined in the UK GDPR and are accordingly Joint Data Controllers within the meaning of the UK GDPR. This joint control is primarily applicable to the personal data of a lay client(s) where the instructing party is my professional client.

Parties

3. This Joint Controllers Data Sharing Agreement ("Agreement") is between:

   (1) Me as a Data Controller

   And

   (2) Any Data Controller instructing me

   (each "a Joint Party" and jointly "the Joint Parties")

Supplemental Agreement

4. This Agreement is supplemental to any other separate contract entered into between the Joint Parties and exists to ensure that there are sufficient security guarantees in place for the safe sharing of personal data and sensitive personal data in accordance with the UK GDPR.

5. Information to which this Agreement relates must be handled in accordance with the appropriate legislative and regulatory environment and each Joint Party's relevant policies and procedures.

Commencement of Agreement

6. This Agreement will commence immediately upon me receiving formal instructions from a Data Controller to carry out any task appropriate for a barrister and upon the transfer of any personal data to me, if transferred prior to formal instruction, and where I and the other Joint Party are Joint Data Controllers.

Length of Agreement

7. This Agreement will remain in place until terminated by either Joint Party and will apply to all cases for all clients that the Joint Parties work on together, now and in the future, unless expressly stated otherwise.

Definitions

8. For the purposes of this agreement "Relevant Information" shall mean any or all personal or sensitive personal data (as defined by the UK GDPR) relating to a client or clients or a case on which the Joint Parties are working together, or the personal or sensitive personal data of data subjects within that client or clients, or connected with the case in question in any fashion.

Purpose and Objectives of the Data Sharing

9. The purpose of the sharing of data detailed in this Agreement is to provide legal advice and representation to the client or clients.

Transfer and Frequency of Data

10. Relevant Information will be shared as and when required for both Joint Parties to discharge their responsibilities to the client(s) and to provide representation in the case appropriately.

Access & Security

11. Under no circumstances should Relevant Information be left unattended or processed in any way that is unsecure.

12. Each Joint Party shall notify the others as soon as is practicable, and at a maximum within five working days, if they become aware of any unauthorised or unlawful processing, loss, damage or destruction of the Relevant Information. This includes any 'near misses' and any incidents reported to the ICO. It is the responsibility of the Joint Party managing the incidents to investigate, report and escalate them as appropriate to the necessary regulatory bodies.

13. Relevant Information will be shared on a strict need-to-know basis only and will only be processed by employees or third-party Data Processors of either Joint Party in order for them to perform their duties in accordance with one or more of the defined purposes.

14. Each Joint Party shall ensure that any processor, agent or subcontractor instructed by them to process Relevant Information will process such information in accordance with the UK GDPR, and that all appropriate data sharing or processing agreements or contracts are in place.

15. Each Party will ensure that all staff with access to the Relevant Information have received appropriate data protection or information governance training and are aware of the confidential nature and duties placed on those processing such information. This includes ensuring they have appropriate monitoring policies and procedures in place for all staff.

16. Failure to meet the standards within this Agreement will result in Relevant Information not being shared, which could result in the termination of this and other service agreements.

Processing of Relevant Information

17. Each Party remains responsible for the Relevant Information held and processed within their own systems.

18. Each Joint Party will ensure Relevant Information will not be processed outside of the UK, and, where relevant, outside of the EEA without the appropriate safeguards being in place to satisfy the UK GDPR.

19. Each party will comply fully with the UK GDPR and other relevant legislation. Particular attention must be paid to Principle 6 and ensuring the security of Relevant Information and systems. Each Joint Party will protect such information from unauthorised or unlawful processing, accidental loss, destruction or damage, and acknowledge that they have implemented the required technical and organisational measures.

UK GDPR and the Freedom of Information Act 2000 Subject Access Requests

20. Each Party is responsible for complying with complaints, queries and objections regarding Relevant Information sharing, subject access and freedom of information requests directed to their respective organisation in line with the relevant legislation or policies in practice. Each individual request must be dealt with on a case by case basis and the consequences of their decisions (for example, to object to sharing) must be clearly explained to the individuals in writing by the party receiving the request.

21. Each Party shall inform the other of any data subject access requests made in respect data which is jointly controlled.

Retention periods

22. Relevant Information will be retained in line with each party's data retention policy, which both parties confirm meets the requirements under the UK GDPR.

Disposal of information

23. Both Parties are individually responsible for deleting or safely disposing of Relevant Information when it is no longer required in line with their own data protection policies, which both parties confirm meet the requirements of the UK GDPR.

Termination and Variation

24. Any Party may terminate this Agreement by giving one calendar month's notice in writing to the other Parties. The terms of this agreement remain binding on any information shared and retained throughout its lifecycle, irrespective of whether the party remains a current signatory to this agreement.

25. Any proposed changes to the Parties involved in this Agreement, to the purposes of the information sharing, the nature or type of information shared or manner in which the information is to be processed and any other suggested changes to the terms of this Agreement must be notified immediately to key contacts within each party so that the impact of the proposed changes can be assessed.

26. This Agreement shall be governed and construed in accordance with English Law and the parties agree to submit to the exclusive jurisdiction of the Courts of England and Wales.

Schedule 2 – Data Controller and Data Processor Agreement

This Agreement is effective as between me and any Data Processor instructed or contracted by me to carry out any form of data processing.

This Agreement is deemed to be dated on the date instructions are received, or a contract for services is formed.

Introduction

1. I will instruct Data Processors to act to process personal data for which I am the applicable Data Controller.

2. Because the services require the processing of personal data and sensitive personal data, the UK GDPR is engaged. I remain the Data Controller and legally responsible for that data processing under the UK GDPR.

3. The 6th Principle of the UK GDPR requires a Data Controller, when using the services of another organisation or company to process personal data on their behalf (a Data Processor), to:

    a) Choose a Data Processor which can provide sufficient guarantees about their data security measures to protect the personal data they will be processing as part of the contract
    b) Take reasonable steps to make sure those security measures are in place and sustained
    c) Document what the Data Processor is allowed to do with the personal data in a written contract. The contract must include: what they can and what they cannot do with the personal data; what security measures must be in place to protect the data; what procedures must be followed if there is a data breach; and any other arrangements i.e. sub-contracting, termination of contract etc. that needs to be included to secure and control the data, including the requirement for the Data Processor to comply with obligations equivalent to those imposed on the Data Controller by the 6th Principle.
    d) Take steps to ensure that: the personal data remains protected; the liabilities and

risks are appropriately managed; data is processed lawfully; and the contract is legally enforceable.

e) Not allow processing of personal data unless the processing is carried out under the written contract, and only when the Data Processor is instructed to process personal data by the Data Controller.

4. As a Data Controller, I wish to engage the services of the Provider as a Data Processor to process personal data which I control as a Data Controller.

Parties

5. This Data Controller and Data Processor Agreement ("Agreement") is between:

(1) Me, as a Data Controller

And

(2) Any Data Processor (within the meaning of the GDPR) instructed or contracted by me to provide services where personal data controlled by me is processed ("the Provider")

(each "a Party" and jointly "the Parties")

Supplemental Agreement

6. This Agreement is supplemental to any other separate contract entered into between the Parties (a "Main Contract") and exists to ensure that there are sufficient security guarantees in place for the safe processing of personal data and sensitive personal data in accordance with the UK GDPR.

7. Information to which this Agreement relates must be handled in accordance with the appropriate legislative and regulatory environment and each Party's relevant policies and

procedures.

Commencement of Agreement

8. This Agreement will commence immediately upon me sending instructions to, or contracting with, the Provider to carry out any task involving the processing of personal data and upon the transfer of any personal data to such a Data Processor in any event.

Length of Agreement

9. This Agreement will remain in place until terminated by either Party or until the Provider ceases to process personal data for me under any Main Contract.

Data Controller Rights and Responsibilities

10. I am the Data Controller of the personal data and are responsible for ensuring it is processed fairly and lawfully and in accordance with the GDPR.

11. Under the UK GDPR, it is the legal duty of a Data Controller to ensure the data protection Principles are met when personal data he or she controls is processed, unless an exemption applies.

12. I remain legally responsible for the data processing carried out by the contracted Provider as Data Processor.

13. I shall not instruct the Provider to process personal data under this Agreement where there is not a secure basis in law for that data to be processed.

14. As the Data Controller, I am entitled during the term of this Agreement to require the Provider to provide reasonable assurances that technical and organisational security measures adequately protect the personal data it is contracted to process.

Data Processor Responsibilities

15. As a Data Processor the Provider shall at all time process personal data only as instructed to do so by me as the Data Controller and in accordance with the UK GDPR and this Agreement.

16. The Provider shall have in place appropriate technical and organisational security measures that protect the personal data it is contracted to process on behalf of the Data Controller from unauthorised or unlawful processing, accidental loss, destruction or damage.

17. The Provider shall provide reasonable assurances and guarantees to me as required that those technical and organisational security measures in place are both appropriate and effective in protecting the processing of personal data.

18. The Provider agrees to maintain good information governance standards and practices, by meeting or exceeding the data protection requirements relevant for its services.

19. The Provider shall not share the personal data with any third party without my prior written permission or process personal data in any way or for any purpose that has not been instructed and authorised by me, or sub-contract a third party to process my personal data without my prior knowledge and written agreement, and only then having provided all the necessary assurance and guarantees of their adequate organisational and technical security measures.

20. The Provider shall not transfer or permit the transfer of the personal data on to any territory outside the UK, and where relevant, outside the EEA, without my prior knowledge and written agreement.

Data Security Requirements

21. The Provider shall:

a) Have regard to the state of technological development and to the cost of implementing any measures, provide a level of security (including appropriate technical and organisational measures) appropriate to the harm that might result from unauthorised or unlawful processing of personal data or the accidental loss, damage or destruction of personal data and the nature of that personal data.

b) Ensure that access to the personal data is limited to those employees who need access to meet the Provider's obligations under this Agreement.

c) Take reasonable steps to ensure the reliability of their personnel who have access to my controlled personal data, which shall include ensuring that all staff engaged by the Provider: understand the confidential nature of the personal data; have received appropriate training in data protection prior to their use of the data; and have signed a written undertaking that they understand and will act in accordance with their responsibilities for confidentiality under contract.

d) Ensure that it has properly configured access rights for its staff, including a well-defined starters and leavers process to ensure appropriate access control.

e) Ensure that suitable and effective authentication processes are established and used to protect personal data.

f) Ensure that the personal data is backed up on a regular basis and that any back-up data is subject to vigorous security measures as necessary to protect the availability, integrity and confidentiality of the data.

g) Implement robust and tested business continuity measures to protect the confidentiality, integrity and availability of my controlled personal data.

h) Encrypt data transferred electronically in accordance with national standards.

i) Ensure that employees are not able to access data remotely, e.g. from home or via their own electronic device or internet portal, other than through a secure electronic network and in accordance with Chambers' Policy.

j) Only dispose of data securely and confidentially when it requires disposal.

Information Breach Incident Reporting

22. The Provider shall have procedures in place to monitor access and to identify unauthorised and unlawful access and use of personal data.

23. The Provider shall immediately report to me any information security incidents relating to a personal data subject whose personal data controlled by me and undertakes to also fully cooperate with my incident investigation requirements.

24. It is my responsibility as Data Controller to ensure that the incident is reported in accordance with the law and informing the relevant data subjects as appropriate.

Secure Destruction

25. The Provider shall ensure that personal data held in paper form (regardless of whether originally provided by me or printed from the Provider's systems) is destroyed using a cross cut shredder or subcontracted to a confidential waste company.

26. The Data Processor shall ensure that electronic storage media used to hold or to process personal data is destroyed or overwritten when no longer in use.

27. In the event of any bad or unusable sectors on electronic media that cannot be overwritten, the Provider shall ensure complete and irretrievable destruction of the media itself.

28. The Provider shall provide me with copies of all relevant overwriting verification reports and/or certificates of secure destruction of personal data at the conclusion of the contract, if requested.

Variations

29. Any variation to the terms of this contract shall be agreed in writing by the Parties and in accordance with the contract management conditions set out in any Main Contract.

Dispute Resolution

30. The Parties shall aim to resolve all disputes, differences and questions by means of co-

operation and consultation and in accordance with any dispute resolution process specified in the Main Contract.

Termination

31. I may terminate this Agreement with immediate effect by written notice to the Provider on or at any time after the occurrence of an event that gives rise to an information security incident or otherwise poses a risk of non-compliance with the data protection principles.

32. Upon this Agreement ending the Provider shall securely return any personal data held or make arrangements for its secure destruction upon being instructed to do so by me.

Schedule 3 – Retention Schedule

This schedule provides category-specific retention periods consistent with UK GDPR principles of storage limitation, data minimisation and accountability.

My retention periods follow Chambers' category-based Retention Schedule, reflecting purpose and legal obligations including guidance from my insurer the Bar Mutual Indemnity Fund. Data is not kept longer than necessary.

Document hold suspension[2] applies where litigation or regulatory action is anticipated.

1. **General case files**
   Standard retention: up to 15 years where necessary for ongoing legal rights or obligations.
   Client contact information retained while case active then reviewed annually.

2. **Sensitive evidence**
   Retain only minimally and no longer than necessary.
   Earlier deletion permitted when no longer required for legal or regulatory purposes.

3. **Complaints/regulatory correspondence**
   Complaints retained 6 years from closure unless escalation requires longer.
   Regulatory correspondence retained at least 7 years.

4. **Financial records**
   At least 7 years.

5. **Pupil/mini-pupil data**
   Pupillage records: 6 years
   Mini-pupils: 6 years unless safeguarding requires longer.

[2] A document hold suspends all deletion. It applies when litigation, investigation or regulatory action is anticipated.

Schedule 4 – BYOD Requirements

I may use a Self-Managed Device only under an executed BYOD Agreement and only where equivalent security can be maintained.

Minimum Security Controls

- Full-disk encryption using industry-standard algorithms (AES-256 or equivalent).
- Mandatory PIN/password/biometric authentication.
- Automatic screen lock after no more than 2 minutes inactivity.
- Supported operating system with all high/critical patches installed within 14 days.
- Active firewall and anti-malware protection running at all times.
- Remote-wipe or remote-lock capability enabled where technically feasible.

Usage Restrictions

- Device must not be “jailbroken”, rooted, or modified to circumvent security controls.
- No shared accounts; no family or third-party access to the device’s Chambers data.
- No automatic cloud synchronisation except approved secure platforms.
- Loss or suspicion of compromise must be reported immediately to Chambers.

Schedule 5 – Breach Workflow

This workflow applies to all breaches affecting data controlled by me.

All communication in relation to any data breach will be informed by the following:

- Ensure that every person provided with information about the incident understands the need for confidentiality.
- Ensure that there is a clear communication strategy with a central point of contact.
- All communications relevant to the incident should be restricted to an agreed group of people to avoid any unintended waiver of privilege or other unplanned disclosure of information.

Step 1 – Identification

- Upon discovering a breach or suspected breach I will report it immediately to Chambers (Chambers' DPO, the Senior Clerk and Heads of Chambers).
- I will not attempt to hide, delete or alter compromised data.
- I will record details of the data breach considering the following:
  When did the incident happen?
  How did the incident happen?
  Has there been any delay between the breach happening and the breach being investigated?
  What is the scope of the breach?
  What data has been breached?
  How many data subjects are affected?
  Are any of the data subjects at risk as a result of the breach?
  What type of information is involved? Is it commercial or personal?
  What can happen to the information? How could it be used to a detrimental effect?
  What action could be taken to deal with those effects?
  If data has been lost or stolen, are there any safeguards in place such as encryption?

Step 2 – Containment & Recovery

- I will contact IT support to isolate affected systems, accounts or devices depending on the technical systems that have been affected.
- If possible, I will recover lost data and prevent further unauthorised access.

Step 3 – Assessment

- I will evaluate risk to individuals' rights and freedoms.
- Factors include sensitivity, identifiability, volume, and potential harm.

Step 4 – Notification

- I will notify affected individuals without undue delay where high risk exists.
- I will notify the ICO within 72 hours where risk is likely.

Step 5 – Documentation & Review

- I will log all incidents and keep a record.
- Lessons learned will be acted upon.

Schedule 6 – Data Protection Impact Assessment (DPIA) Template

I will refer to the following template for any processing likely to result in high risk to individuals.

1. Project/Processing Name

- Describe the activity and its purpose.

2. Description of Processing

- What data is collected?
- How is it stored, accessed and transferred?
- Who are the recipients or categories of recipients?

3. Lawful Basis and Article 9/10 Conditions (if applicable)

- Identify relevant bases and special category/criminal data conditions.

4. Necessity and Proportionality

- Explain why the processing is needed and proportionate to aims.

5. Risks to Individuals

- Unauthorised access, loss, misuse, inaccuracy, discrimination, distress.

6. Measures to Reduce Risks

- Technical, organisational and contractual safeguards.

7. Review & Sign-Off

- If consulted, any comments from Chambers' DPO or other relevant person.
- Final decision and date recorded.

Schedule 7 – Document hold Procedure

A document hold prevents deletion or alteration of records relevant to litigation, investigations or regulatory action.

Trigger Events

- Receipt of a claim, complaint or regulatory inquiry.
- Reasonable anticipation of litigation or investigation.

Steps

- Identify relevant custodians, data sources and systems.
- Suspend deletion, auto-purge and overwrite routines.
- Inform all custodians of responsibilities and restrictions.
- Monitor compliance and maintain an audit trail.

Release of Hold

- Hold is lifted only when the circumstances reasonably indicate that it is safe to do so.

Schedule 8 – Cloud Security Standards

These standards apply to any cloud service used to store or process data controlled by me, including my practice data where Chambers is IT provider.

Provider Due Diligence

- Review data location, certifications (ISO 27001), availability SLAs and incident reporting duties.
- Ensure provider offers contractual commitments on confidentiality, security and deletion.

Technical Requirements

- Data encrypted in transit and at rest with strong cryptography.
- Access restricted using MFA and role-based permissions.
- Audit logging and monitored administrator activity required.

International Transfers

- Before any cloud provider stores/processes UK personal data outside the UK/EEA, I must confirm: (i) adequacy applies (e.g., UK-US Data Bridge with DPF UK Extension listing), or (ii) IDTA/UK Addendum is in place and a TRA has been completed with any extra technical/contractual controls applied.
- Complete transfer risk assessments and document decisions.

Off-Boarding

- Provider must delete or return data securely at contract end and provide written confirmation.