DATA PROTECTION POLICY

Introduction

1. I am a Data Controller under the General Data Protection Regulation (GDPR) and am registered with the Information Commissioner's Officer as a Data Controller.
2. Compliance with the GDPR is overseen by the UK data protection regulator which is the Information Commissioner's Office (ICO). This Practice is accountable to the ICO for its data protection compliance.

Purpose

3. This policy aims to protect and promote the data protection rights of individuals, by informing everyone working for Lucy Coulson of their data protection obligations and of the procedures that must be followed to ensure compliance with the GDPR.

Scope

4. This policy applies to Lucy Coulson and any third party that this policy has been communicated to.

5. This policy covers all personal and sensitive personal data, processed on computers or stored in manual (paper based) files.

Responsibility

6. I am responsible for this policy and for monitoring compliance with this policy.

7. In the case of any queries or questions in relation to this policy please contact me, Lucy Coulson.

8. I recognise that I control and am personally responsible for compliance with the GDPR in relation to the personal data that I control, which is all the personal data coming to me in the course of my practice. I recognise this as a non-delegable responsibility. I do not process data for clients.

9. Employees of and contractors employed by No5 Chambers Limited will have access to some of the data which I control. Although I recognise the non-delegable nature of my responsibility, having considered No5 Chambers Limited's own policies I consider that those policies are adequate and appropriate. I therefore do not intend to lay down any further or different policies in respect of such employees and contractors.

10. Data controlled by me will sometimes be shared with other data controllers, such as solicitors and other barristers. Where such other professionals are under a regulatory obligation of their own to comply with the GDPR, I will not investigate their compliance but will assume they will comply with their duties unless there is any reason to suggest otherwise.

11. In the case of data processors who are not employees of No5 Chambers or are not professionals subject to their own regulation as aforesaid, I will ensure that everyone processing personal data which I control understands that they are responsible for following best data protection practice, are appropriately trained to do so and are appropriately supervised. Where appropriate, I will enter into data processing agreements to promote best data protection practice by those to whom I entrust data.

GDPR

12. The GDPR is designed to protect individuals and personal data which is held and processed about them by organisations or other individuals.

13. The GDPR uses some key terms to refer to individuals, those processing personal data about individuals and types of data covered by the Act. These key terms are:

Data subject

Means any living, identified or identifiable individual who is the subject of personal data i.e. the person that the personal data is about.
For the Practice's purposes, our lay clients are data subjects (other individual third parties that we hold personal data about are also likely to be data subjects).

Data controller

Means a person who (either alone, or jointly, or in common with other persons) determines the purpose for which and the manner in which any personal data are, or are to be, processed.
I.e. data controllers can be individuals; organisations; or other corporate and unincorporated bodies of persons.
For the Practice's purposes, this Practice is a data controller.

Processing

Means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including –
(a) organisation, adaptation or alteration of the information or data;
(b) retrieval, consultation or use of the information or data;
(c) disclosure of the information or data by transmission, dissemination or otherwise making available; or
(d) alignment, combination, blocking, erasure or destruction of the information or data.
For the Practice's purposes, everything that we do with client information (and personal information of third parties) is 'processing' as defined by the GDPR.

Personal data

Means data which relate to a data subject who can be identified, or is identifiable, directly or indirectly:
(a) from those data; or
(b) from those 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. Personal data includes sensitive personal data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed.

For example: name; date of birth; address; employment and education history; video footage; photographs, IP addresses, mobile device IDs etc.

Sensitive personal data

Means personal data consisting of information as to:
(a) the racial, or ethnic origin, of the data subject;
(b) his political opinions;
(c) his religious beliefs, or other beliefs of a similar nature;
(d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992);

(e) his physical, or mental health, or condition;
(f) any genetic or biometric information (where used to identify an individual);
(g) his sexual life or sexual orientation;
(h) the commission, or alleged commission, by him of any offence; or
(i) any proceedings for any offence committed, or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

This data is also called special categories of personal data in the GDPR

Data Protection Principles

14. The GDPR is based around 6 principles which are the starting point to ensure compliance with the regulation. Everybody working for Lucy Coulson must adhere to these principles in performing their day-to-day duties. The principles require the Practice to ensure that all personal data and sensitive personal data are:

(1) fairly and lawfully processed in a transparent manner;
(2) processed for limited purposes;
(3) accurate and where necessary kept up to date;
(4) not kept longer than necessary;
(5) made available to data subjects and processed in accordance with the data subject's rights;
(6) secure; and not transferred to countries without adequate protection.

Processing personal data

15. I will process all personal data in a manner that is compliant with the GDPR, in short, this means I will:

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

16. I will ensure that you are aware of the difference between personal data and sensitive personal data and ensure that both types of data are treated adequately.

Processing sensitive personal data

17. You must process all sensitive personal data in a manner that is compliant with the GDPR, in short, this means you must only process sensitive personal information when:

- You have given explicit, written consent of the data subject;
- It is in the public interest, such as for equal rights monitoring or in relation to an occupational pension scheme;
- You need the information to carry out a legal obligation;
- It is necessary to protect the data subject;
- The data subject has made the information public.

18. I will process personal data lawfully within the meaning of Art 6, and fairly and transparently.

19. When instructions have been received and work upon them is not yet complete, I will collect, retain, access, use and communicate the data for the purpose of delivering my services.

20. When instructions have been fulfilled, I will retain the data only for one or more of the Art 6 reasons: essentially to meet my business needs (to enable me to provide a better service if instructed again in relation to the same or a related matter), to comply with

legal requirements, to provide evidence in the event of disputes and/or in the defence of a legal claim.

21. I will collect data only for the purpose of delivering legal services in my practice as a barrister.

22. I will not further process data in a manner incompatible with that purpose.

23. I will collect and process adequate and relevant information, and only to the extent that it is needed for the purpose identified above. However I will take a practical approach to this. I will not sift every document delivered to me and delete those parts which are not strictly necessary for the case on which I am working. It would not be practicable to do so. I will trust professionals and lay clients providing me with data to provide only what is reasonably necessary.

24. I may use personal data for the following purposes:

- to provide legal services to my clients, including the provision of legal advice and representation
- to keep accounting records and carry out office administration
- to take or defend legal or regulatory proceedings or to exercise a lien
- to respond to potential complaints or make complaints
- to check for potential conflicts of interest in relation to future potential cases
- to promote and market my services
- to carry out anti-money laundering and terrorist financing checks
- to train other barristers and when providing work-shadowing opportunities
- to respond to requests for references
- when procuring goods and services
- as required or permitted by law.

25. I will ensure that so far as it is necessary and within my reasonable power to do so, the personal data is kept up to date. The nature of my practice requires certain personal data to be the subject of contention.

26. I will keep personal data only so long as the purposes identified above persist.

27. I will take appropriate technical and organisational security measures to safeguard personal data

28. I will not transfer information outside the UK except by communicating it to a client or his/her/its authorised representative abroad.

29. I will set out clear procedures for responding to requests for information.

30. I will ensure that the rights of people about whom information is held, can be fully exercised under the GDPR.

Data Storage and access

<u>The data</u>

31. The data I control may be divided into the following groups, according to how and where it is kept. This categorisation is not intended to be exhaustive but is intended to assist in achieving the security objectives identified below:

- Hard copy documents
- Electronic files (pdf, Word, spreadsheets, jpegs, PowerPoint etc) stored digitally on OneDrive Business and downloaded via OneDrive Business on my electronic devices.
- Documents open for Emails - Emails to and from clients which will often include case information and correspondence. I receive, send and store emails in Mail on my iMac, MacBook Air iphone and ipad.
- Contact details of clients including personal data such as name/address and financial information relating to billing. This data is kept for me by No5 Chambers and 18 St John Street Chambers (in relation to work undertaken whilst at 18 St John Street Chambers).

The devices

32. The devices which I use to access this data are:
    - An Apple iMac which I keep at home
    - An Apple MacBook which I often carry with me when out of chambers and away from home
    - An Applie iPad which I often carry with me when out of chambers and away from home
    - An iPhone which is usually with me
    - A Windows Laptop which I usually keep at home but occasionally may carry with me away from home for business purposes.

33. I occasionally receive data from solicitors or lay clients on external media such as USB sticks, CDs or DVDs. Occasionally I may wish to copy data to external media. I do not retain such external media beyond what is necessary for a case and will save such data to No5 Chambers' Dropbox.

Third parties

34. I share data with No5 Chambers and its staff. I do not have a formal data sharing agreement with my chambers because I have total confidence in the integrity of its systems and of its senior management and I understand as a legal organisation that it has taken reasonable steps to ensure that its systems and policies are compliant.

35. Occasionally employees of Cloud Systems access my devices for maintenance and similar purposes, but only in my presence and under my supervision.

36. I share data related to billing and accounting with 18 St John Street Chambers and its staff in relation to work undertaken between 2016 – 2021. 18 St John Street Chambers also retain data related to work undertaken in this period on their computing system Lex. I do not have a formal data sharing agreement with my chambers because I have total confidence in the integrity of its systems and of its senior management and I understand as a legal organisation that it has taken reasonable steps to ensure that its systems and policies are compliant.

Security
Objectives

37. My security objectives are to ensure:
    - Confidentiality of information – access to information is restricted to those persons with appropriate authority to access it
    - Integrity of information – information shall be complete and accurate.

- Availability of information – information shall be available and delivered to the right person at the time when it is needed.

Hardcopy documents

38. I only occasionally need papers with me wherever I am working, which might be in chambers, at home, in court, at others' offices (particularly solicitors' offices), while travelling or in hotels.

39. All papers will be moved securely between these locations. On public transport they will not be left unattended out of my bag. Papers left in an unattended car will be stored out of sight. This will only occur where necessary and for brief periods of low risk. Case files will not be left in a car overnight.

40. Papers will never be left freely available in any common area in circumstances where there is a real risk that they may be read by unauthorised individuals. They will never be opened in circumstances where there is such a risk.

41. I only take papers home for the purpose of working on them so they remain outside chambers no longer than reasonably necessary. They are kept in my private study. When papers are not in use but are at home they are left in a locked filing cabinet in the study.

42. Given the nature of my practice, I am satisfied that my home is unlikely to be targeted for the purpose of stealing personal data.

Electronic files in No5 Chambers' Dropbox account

43. This account is administered on behalf of No5 Chambers by Cloud Systems and is fully secure. The integrity and accessibility of data is assured.

44. I use the No5 Chambers Dropbox to access and store papers.

Electronic files in OneDrive Business account
t

45. This account is administered by Microsoft and is fully secure. The integrity and accessibility of data is assured.

46. From time to time I transfer and temporarily store papers on OneDrive Business from the No5 Chambers Dropbox.

47. I store documents created by me on my OneDrive Business Account (for example pleadings, attendance notes, advice).

48. I also store papers and documents created by me for work between 2016 – 2021, whilst a member of 18 St John Street Chambers, on my OneDrive Business Account. Where I continue to work on a case at No5 Chambers, I may transfer this data to the No5 Chambers' Dropbox account.

Files being access and/or accessible from my devices

49. Electronic files will never be opened on a screen in circumstances where they can be read by members of the public. In the event that they are open on a screen when

unlocking my Mabook Air, ipad or iphone personal data contained within any such file is kept limited to what is necessary and not left on the screen for anything but a brief period of time. Where appropriate, I use a privacy screen on my devices.

50. All the devices identified above will be kept secure at all times within the limits of reasonable practicability.

    a. The phone is password protected and encrypted.

    b. The ipad is password protected using Apple software. It is also encrypted. It locks automatically when not used. It will not be left unattended and on view. It will only be left unattended at all where this is not reasonably avoidable.

    c. The Mac is password protected using Apple software. It is also encrypted. It locks automatically after 5 minutes. It is kept at home.

    d. The MacBook Air is password protected using Apple software. It is also encrypted. It locks automatically after 5 minutes. It will not be left unattended and on view. It will only be left unattended at all where this is not reasonably avoidable.

    e. The Windows Computer is password protected using Windows Software. It is also encrypted. It locks automatically. It will not be left unattended and on view. It will only be left unattended at all where this is not reasonably avoidable.

51. The devices are kept up-to-date with software updates to ensure security is maintained.

52. Operating software is checked regularly to ensure that the latest security updates are downloaded.

53. Removable storage media such as memory sticks will be rarely used. I do sometimes accept documents on such media and rarely may load documents onto them. On such occasions the memory stick will be guarded as carefully as all other devices containing personal data and returned to chambers as soon practicable after I am finished with it.

Rights of the data subject

54. All data subjects have the right to access the information I holds about them, except where specific exemptions apply.

55. I will deal with subject access requests in accordance with the Subject Access Request Policy of No5 Chambers.

56. The GDPR gives rights to individuals in respect of the personal data that organisations hold about them.

57. The rights of data subjects include:

    - a right of access to a copy of the information comprised in their personal data. This enables the data subject to receive a copy of the personal information we hold about them and ensure we are lawfully processing it;
    - a right to request correction of the personal information we hold. This enables the data subject to have any incomplete or inaccurate information we hold about them corrected;

- a right to request erasure of their personal information. This enables the data subject to ask us to delete their personal information where there is no good reason for us to continue processing it, or if they object to processing (see below);
- a right to object to the processing of their personal information where we are relying on a legitimate interest (or those of a third party) and there is something about their particular situation which allows them to object to processing on this ground;
- a right to prevent processing for direct marketing;
- a right to object to decisions being taken by automated means;
- a right to complain to a supervisory authority;
- a right to withdraw consent;
- a right to claim compensation for damages caused by a breach of the Act.

58. If anybody receives a request from a data subject (a client or other third party that we hold personal data about) to exercise any of these rights, the request must be referred to me immediately, or to No.5 Chambers in my absence.

59. If you want to exercise any of these rights, please:

- Email me: Lucy Coulson - lco@no5.com
- Provide information so that I can identify you, for example; a copy of your Passport, Driver's License, Utility Bill etc. I may need to contact you to request further information to verify your identity;
- Let me have proof of your identity and address;
- State the right or rights that you wish to exercise.

I will respond to you within one month from when I receive your request.

Note: I only have one month to respond to a request to access a copy of personal data.

Storage and Retention of Information

60. I will only retain personal information of data subjects for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements.

61. Notwithstanding the general principle above, the following general principles apply:

a) My policy is to retain electronic data for at least 6 years. I consider it proportionate to retain for that period since the possibility of a dispute may endure for 6 years from the date of the last work undertaken.

b) Further, data in cases involving children (aged 18 or under), for whom limitation within the meaning of the Limitation Act 1980 does not run until they turn 18 years old I will retain until at least 6 years after limitation has started to run. I will endeavour to delete such documents within a reasonable timescale after that point.

c) Further, data in cases involving Protected Parties (those who lack capacity to litigate and for whom limitation does not run) I will retain electronic data for 15

years, such time being a reasonable and proportionate time to ensure that any legal claim that can be reasonably envisaged can be defended. I will endeavour to delete such documents within a reasonable time scale after that point.

62. As to paper documents, these will be returned to instructing solicitors or other professional clients when I no longer need to keep them for the purposes of working on the case. The solicitors are entitled to their return and will have their own professional obligations and retention policies. Papers may be retained whilst awaiting the outcome of any given case/confirmation that the papers are no longer required/payment has been provided. I will ensure that each year the paper documents retained are evaluated to enable their destruction or return as appropriate.

63. Paper documents will only be retained in No5 Chambers' premises, wherever those may be from time to time. They may be brought home for the purposes of working on and preparing cases but will be returned to chambers' premises as soon as practicable and proportionate.

64. Where I have created paper documents by printing copies of electronic documents, I may retain these until paperwork is complete or a case is finished. I will retain any such documents for a reasonable and proportionate period of time. Ordinarily, such documents will be disposed of confidentially (e.g. by shredding), promptly after use. From time to time, it is desirable to retain such documents for a longer period in order to fulfil my work tasks.

65. 6. However none of the above paragraphs are definitive. I will keep individual cases under review. The ultimate disposal decision will have regard to:

    - on-going business and accountability needs (including audit);
    - current applicable legislation;
    - whether the record has any long-term historical or research value;
    - best practice in the profession;
    - costs associated with continued storage.

66. No destruction of data will take place unless:

    - the data is no longer required for the purpose of my practice;
    - no work is outstanding;
    - no litigation or investigation is current or pending which affects the data;
    - there are no current or pending FOIA or GDPR subject access requests which affect the data.

Breaches

67. A personal data breach is 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.

68. I will report any actual, or suspected, personal data breach without delay.

Complaints

69. Complaints relating to breaches of the GDPR and / or complaints that an individual's personal data is not being processed in line with the data protection principles should be referred to me without delay.

HOW TO MAKE A COMPLAINT?

70. I hope that you are happy with the service I provide and that I can resolve any issues or complaints that arise. Please get in touch with me or with Robert Woods, the Data Protection Manager robertw@no5.com if you have any concerns.

71. The General Data Protection Regulation also gives you the right to lodge a complaint with a supervisory authority. The UK supervisory authority is the Information Commissioner's Office who can be contacted at https://ico.org.uk/concerns/.

CONTACT ME

72. If you have any questions about this privacy notice, or the information I hold about you, please contact me directly and we will happily discuss this with you.

    The best way to reach me is to contact me by email: lco@no5.com

ALTERNATIVE FORMATS

73. If it would be helpful to have this notice provided in another format (for example: in another language, audio, braille) please contact me.

Training

74. I will ensure that I am appropriately trained in Data Protection. This has included the No5 Rilliance GDPR Training package which I undertook in January 2021.

Monitoring compliance

75. Compliance with this policy will be managed by investigating all data protection breaches and complaints.

Review of this policy

76. This policy will be reviewed at least annually. The next review is due on, or around November 2024.

Record of review

Version	Date of review	Reviewer	Comments/amendments required	Date of next review
1	Jan 2022	LCO	1st Edition	Jan 2023
2	Nov 2021	LCO	2nd Edition – minor amendments to clarify parts of policy.	Nov 2023
3	Nov 2022	LCO	3rd Edition – no substantive amendments	Nov 2024

DATA PROTECTION BREACH REPORTING PROCEDURE

Our responsibility

Lucy Coulson is responsible for ensuring that personal data processed is not:

- Accessed without authority;
- Processed unlawfully;
- Lost;
- Destroyed; or
- Damaged.

What is a data protection breach?

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.”

Data protection breaches can happen for a wide range of reasons, including:

- Human error;
- Cyber-attacks;
- Loss or theft of devices or equipment on which personal data is stored;
- Inadequate or inappropriate access controls;
- Deceit; and
- Disasters at Practice premises i.e. fire or flood.

If you are unsure whether a particular circumstance or incident constitutes a data protection breach, please refer the matter to Lucy Coulson or another suitable person in their absence for guidance.

Reporting a personal data breach

All personal data breaches must be reported to Lucy Coulson immediately upon discovery.

Reports should be made by filling in the form in this policy.

Managing data protection breaches

There are four key steps to our data protection breach management plan:

1. Containment and recovery
2. Assessment and ongoing risk
3. Notification of breach
4. Evaluation and response

1. Containment and recovery

Lucy Coulson must:

- Take steps to recover any lost data and limit the damage that the breach can cause where possible;
- Decide who will lead the investigation into the breach; and

- Find out who needs to be aware of the breach and tell those persons what they are expected to do (if anything) to assist in the containment and recovery of the breach.

2. Assess the risks

Lucy Coulson must assess the potential adverse consequences of the breach for the individuals concerned (the people that the personal data in question belongs to), the potential severity, or scale of the breach, and the likelihood of the adverse consequences occurring.

3. Notification of breaches

Lucy Coulson has a duty to report all data protection breaches that are likely to result in a risk to the rights and freedoms of individuals to the Information Commissioner's Office (ICO).

Lucy Coulson is responsible for ensuring that all relevant data protection breaches are reported to the ICO without delay and no later than 72 hours after having become aware of it.

Lucy Coulson will report the breach to the ICO in accordance with the reporting methods set by the ICO.

Where deemed appropriate, the individuals affected by the data protection breach must also be informed. Lucy Coulson must provide individuals with specific and clear information about what has happened and what is being done to address the breach. Advice should also be offered on any steps that the individual can take to protect themselves. The individuals must be given contact details should they require further information or help.

Considerations must also be made as to whether any other third parties should be notified i.e. the Police, insurers, professional bodies, the bank etc.

4. Evaluation and response

It is important to establish whether the breach was caused by an isolated incident, or is part of a wider systematic issue, so that we can try to stop the same, or a similar breach, from occurring in the future.

Any lessons learned should be shared.

Lucy Coulson will review all any records of data breaches periodically to establish any trends requiring further attention.

Recording a data protection breach

Lucy Coulson is responsible for maintaining a data protection breach register.

Review of this procedure
This procedure will be reviewed at least annually by Lucy Coulson. The next review is due on, or around November 2023.

Record of review

Version	Date of review	Reviewer	Comments/ amendments required	Date of next review
V2	November 2022	LCO	No amendments	November 2023

Appendix 1 – Data Protection Breach Report Form

Date	
Name	
Department	
Description of the actual or suspected data protection breach (please provide as much detail as possible)	**What happened?** **When did it happen?** **When did you become aware of it?** **How did it happen?**
Personal data at risk (please provide as much detail as possible)	**What type of personal data is at risk?** I.e. what does the information relate to? **How many individuals have been affected?** **Are these individuals aware of the incident?** **Is anybody else within the Practice aware of the incident?** **Is any third party aware of this incident?**