PENDRAGON CHAMBERS

CHAMBERS DATA PROTECTION AND INFORMATION RISK POLICY/ INFORMATION PLAN

1) This document is prepared as part of the annual Chambers planning process and reviewed on a 12 monthly basis.

2) Pendragon Chambers will complete an information asset register ("IAF") by way of a word document to register all data held which will be updated on an ongoing basis along with all systems used to store and process data and a register of all third parties with which they share data. The IAF will be completed forthwith and continually updated.

3) When completing the IAF the barrister will consider the impact of losing data and how sensitive the data is in relation to GDPR.

4) This document aims to ensure that Pendragon Chambers as a whole, its individual members and its clerks fulfil their obligations to protect data which includes their obligations as a result of the Data Protection Act 1998, the Attorney General's Guidelines on Information Security and Government Work and their own obligations as barristers in accordance with the Code of Conduct for example.

5) This document aims to ensure that Pendragon Chambers as a whole are compliant with the need to protect data. Towards the end of this document there will be general guidance for individual barristers (who are all data controllers in their own right) but this will not necessarily include all matters which an individual needs to consider and all barristers within Pendragon Chambers are encouraged to:

(a) Adopt all of this document in respect of their individual practices, AND

(b) Add to the written document by way of an individual policy document in the event that their own particular practice necessitates additional policies.

6) This document does not replace the need for individual members to put in place particular procedures.

7) The data group which Pendragon Chambers, individual members and clerks hold are as follows:

   a) Physical Case Files

   b) Digital Case Files

   c) Emails

   d) Client Contact Details

   e) Client Financial Details

8) The majority of data retained will be as a result of a legal basis such as providing legal services, establishment, exercise and defence of a legal claim, compliance with a legal obligation or retaining reference materials and record keeping (provided that this right is balanced with the rights of the data subject).

9) In respect of all data groups the following must be adhered to:

   a) Is all data accurate and up to date

   b) Is the data still needed for the purpose documented and is the data minimized

   c) Has consent been given to process data by the data subject

   d) If data is shared or published, does the data subject know this and have they given consent?

   e) Is the processing lawful and fair

   f) Has the data subject been provided information on how data is going to be processed.

10) We do not carry out regular and systematic monitoring of data subjects on a large scale. As a result, in accordance with Article 29 WP guidance on Data Protection Officers we do not currently need to appoint a Data Protection Officer.

11) In the event that the guidance changes, a DPO will be appointed and the following will apply:

    a) The DPO will be nominated from time to time

    b) The DPO does not assume any responsibility for individual compliance and any liability which may arise as a result of a failure to comply with the need to protect data

    c) The DPO will be responsible on a yearly basis for ensuring that the Data Protection Policy is fit for purpose, that all members are registered with the Information Commissioner and for overseeing any breached (unless those breaches apply to the DPO, in which case they will be overseen by a person/ person (s) nominated by Chambers.

12) The Head of Chambers, Sara Rudman ("HoC") and the Practice Manager, Martin Bowen (PM) will be responsible on a yearly basis for ensuring that the Data Protection Policy is fit for purpose, that all members are registered with the Information Commissioner and for overseeing any breaches (unless those breaches apply to either the PM or HoC, in which case they will be overseen by a person/ person (s) nominated by Chambers.

13) It is the responsibility of all members and clerks to seek and update from time to time training, whether by attendance at a training course, online training or in any other way in respect of data protection,

14) Pupils and mini pupils will be given a copy of this policy and asked to sign an undertaking which appears towards the end of this policy ("the pupil/ mini pupil undertaking").

15) Any contractors which Pendragon Chambers use from time to time will be given a copy of this policy and asked to sign the undertaking and indemnity which appears towards the end of this policy (the "contractor undertaking/ indemnity")

16) Pendragon Chambers does not use automated decision making; in the event that this changes, further policies will be implemented.

17) In respect of protection measures in place for data leaving the office these are provided for within the "individual guidance for barristers" section of this policy.

18) Each member of chambers and member of the clerking team is a Data Processor and must abide by this policy and any other safeguards applicable to the individual to ensure that data is protected.

19) In the event that a third party data processor is used, there must be a signed contract with the data processor which protects each individuals processing.

20) All data is processed within the European Economic Area ("EEA"), in the event that a member who processes data outside of the EEA has a contract in place between the data controller and the processor to ensure data security and transfer out of the EEA.

21) A project plan will be completed and reviewed on at least an annual basis (print out template- reliance assets folder

22) Chambers has adequate insurance in place against data breaches, leaks etc collectively. This insurance does not cover individual members for any potential liability arising out of data related breaches and claims. Cover provided by BMIF may not cover any such claim and members are encouraged to seek advice of a professional broker who can assist if they feel that cover through BMIF is not adequate.

23) This document has been approved by all members of chambers and Pendragon Management Services ("the clerks") on the 17th May 2018.

PARTICULARS OF THE POLICY

SECURITY OF CHAMBERS (PREMISES)

1) There is an external door to the building which houses chambers. Entry to that door is by an activated fob or by calling chambers from the door and waiting for entry. In respect of the fobs the following will apply:

   a) Fobs will only be supplied to members of chambers and clerks and when a member ceases to be a member or a clerk withdraws their services from the clerking partnership the fob will be returned forthwith.

b) Fobs will not be given/ loaned to anyone else.

2) Entry to chambers is via a door which outside of chambers "working hours" (8.30 am to 5.45 pm weekdays) shall be kept locked. Entry to that door is by a key and in respect of the key the following will apply:

   a) Keys will only be supplied to members of chambers and clerks and when a member ceases to be a member or a clerk withdraws their services from the clerking partnership the fob will be returned forthwith.

   b) Keys will not be given/ loaned to anyone else.

   c) In the event that a key is mislaid by an individual member the lock must be replaced and all keys forthwith at the expense of the member.

3) When unoccupied Chambers shall be secured and all windows and the doors shall be kept locked.

4) Entry will not be allowed to any individual who chambers are not aware of their identity and their reason for visiting chambers. Upon entry, visitors will remain within the waiting room. All of their reasonable needs will be met within the waiting room.

5) Within chambers, the following shall apply:

a) In the event that members/ other individuals enter chambers the clerks shall ensure that confidential information cannot be seen

b) All individual data shall be kept in locked cupboards within chambers unless the member/ clerk are dealing with those papers. They will either be locked with a combination lock (the number will only be known by the individual barrister and the clerks) alternatively keys shall be kept by individual barristers and it is their responsibility to keep those keys secure.

c) There will be a duplicate key kept within chambers in a secure place for use by the clerks.

d) In the event that a key is mislaid by an individual member the lock and key must be replaced forthwith at the expense of the member.

e) All members and clerks shall ensure that data is not left out in general view where someone may inadvertently read it when entering the room. Data shall only be out of the locked cupboards when it is being worked on.

6) In respect of pigeon holes the following shall apply:

   a) The pigeon holes are not to be used to store information and members must ensure that they transfer material from their pigeon hole to the locked cupboards/ retain for use securely as part of their working practice.

   b) Visitors to chambers who need to enter chambers shall be supervised constantly, in particular near pigeon holes.

7) In respect of photocopiers the following shall apply:

   a) Members will remove printed confidential information as soon as it is printed.

   b) On a regular basis the printer will be checked and any confidential information which has not been collected will be disposed of confidentially.

8) Chambers is open plan beyond the waiting room and the following shall apply:

   a) Members of chambers shall enter chambers during working hours to deliver and collect briefs but will not work within chambers and this will ensure that they do not hear information being discussed by the clerks within chambers which is confidential.

   b) Special measures will be taken in the event that more than one barrister is instructed in the same case to ensure that there is no cross-over of information.

9) In respect of conferences in Chambers, these can continue to take place outside of chambers hours, but it is the responsibility of the individual members to ensure before the attendee leaves the waiting room that there is no confidential material within chambers which an attendee could see.

10) In respect of interviews in Chambers, these can continue to take place outside of chambers hours, but it is the responsibility of the interviewing committee to ensure before the attendee leaves the waiting room that there is no confidential material within chambers which an attendee could see.

SECURITY OF CHAMBERS (INFORMATION TECHNOLOGY)

1) Chambers computers shall only be turned on during working hours and the following shall apply:

    a) Computers will be password protected with a password which is either made of at least 5 letters, a number and a special character or a fingerprint identification and that after a maximum of 10 minutes of non- use the password needs to be re entered.

    b) Computers will have an adequate antivirus, anti- spyware and firewall software program installed

2) Data stored on a removable medium, CD's, USB sticks etc will be kept in the members locked cupboards unless they are particularly sensitive (in relation to sex abuse allegations etc) and then shall be kept in a safe.

3) The following will apply to encryption:

    a) Computers used to store information will be protected using approved encryption software which is designed to guard against the compromise of information

    b) Emails sent via the Chambers server shall be encrypted if they include personal data.

DATA RETAINED

1) In relation to physical case files/ papers the following shall apply:

    a) Bundles shall have only initials on the index of the parties involved, the name of the public body (if there is one) in full along with the solicitors firm

b) The front sheet of files and loose papers shall not include any full names and again merely set out initials and the name of the public body as provided for above.

DELETION OF DATA

1) At the end of each case, wherever possible papers shall be returned to lay and professional clients by means of DX/ Recorded delivery/ post.

2) Alternatively the information shall be disposed of confidentially by way of a confidential waste provider, such as Matthews or by shredding.

3) In relation to direct access clients the information shall be kept (for the limitation period of a potential claim plus one year) within a secure place and at the end of that time the information will be securely disposed of. This retention complies with legal obligations.

4) In relation to blue note books, these will be kept (for the limitation period of a potential claim plus one year) within a secure place and at the end of that time the information will be securely disposed of.

5) All data subjects have the right to request that personal informal is deleted without delay. These data will be erased where the personal data is no longer necessary/ consent is withdrawn and there is no other legal ground for processing or overriding legitimate grounds for processing/ the date has been lawfully processed/ it must be erased to comply with a legal obligation or the date is in relation to the offering of information society services or in relation to a child over 13 years old. Data does not have to be erased if it is necessary to retain it to comply with a legal obligation, for the establishment, exercise or defence of legal claims.

DATA PROTECTION BREACH

1) In the event that a breach of data protection has occurred which is unlikely to result in a risk to the rights and freedoms of natural persons the following shall apply:

a) The breach must be recorded

b) The breach must be notified by the member to the HoC and PM asap and within 72 hours maximum

c) The HoC and PM shall act swiftly to minimize damage

d) Insurance arrangements will be revised

e) The HoC and PM will consider whether the breach should be dealt with by chambers as a disciplinary matter and if so the matter will be referred to a Disciplinary Committee.

f) The HoC and PM will review procedures and consider whether improvements can be made to avoid/ minimize any future repetition of the breach including training

2) In the event that a breach of data protection has occurred which is likely to result in a risk to the rights and freedoms of natural persons the following shall apply:

a) The data controller must without undue delay and no later than 72 hours of having become aware it, notify the personal data breach to the supervisory body and if this notification is delayed it must be accompanied with a valid reason for the delay.
b) The notification shall describe the nature of the breach, a contact detail, the likely consequences of the personal data breach, describe the measures taken to address the breach

c) The data controller must document this breach, effects and remedial action

3) In the event that there is a personal data breach which is likely to result in a high risk to the rights and freedoms of natural persons the following shall apply:

a) If appropriate technical and organizational measures have been taken to render the data unintelligible to those not authorized to see it (eg by means of encryption), measures have been taken so that the high risk is not likely to materialize or if would involved disproportionate effort (eg because of the number of subjects and then public communication etc should be used). If this provisions do not apply then the following must occur:

i) The Data subject must be told without undue delay by the data controller

ii) The communication must be in clear and plan language and contain at least a contact point for more information, the likely consequences of the breach and measures to be taken to address the breach

GIVING AND WITHDRAWING OF CONSENT

1) Valid consent must be given by data subjects to the storage of information and the following will apply:

   a) Once the direct access consent form has been signed by a data subject which will be included in the details form/ the terms and conditions letter has been sent to a data controller, consent has been given

2) In the event that consent is withdrawn, the following shall apply:

   a) The member will consider if they are professionally embarrassed as a result of the withdrawal of consent and if so shall take the necessary steps, if not,

   b) the member shall consider alternative means of lawful processing rather than relying exclusively on consent

SUBJECT ACCESS REQUESTS, RECTIFICATION and RESTRICTION

1) In the event that a request is made for access to data the following procedure will apply

   a) The nominated officer for dealing with subject access requests are the practice manager, Martin Bowen and the Head of Chambers, Sara Rudman who will work together in respect of each subject access request

   b) The data controller will be asked to provide a copy of such information in a machine readable form free of charge, without delay at the latest within one month of receipt provided that the request is in writing/ by email. If the request is manifestly

unfounded or excessive or further copies are requested a reasonable administrative fee may be requested.

2) The data subject has the right to obtain without undue delay the rectification of inaccurate personal data concerning themselves without delay and to have incomplete data completed.

3) The data subject has the right to restrict access if the accuracy is contested by the subject and processing can be restricted until the controller had verified accuracy. Restriction can also occur if the information is not needed but needs to be maintained for legal claims in which case the objection will be weighed against the legitimate grounds of the controller.

4) Rectification and/ or restriction shall be notified to recipients of personal data.

5) Data subjects have the right to object to the processing of personal data and this right to object must be brought to their attention. When dealing with any objection Chambers will consider necessity for the performance of a task or purposes of a legitimate interest but if the objection is in respect of direct marketing then there is an absolute right to object

PRIVACY NOTICES

1) All clients, data subjects other than clients (including anyone who communicates with a barrister by electronic means such as email, SMS message and twitter such as solicitors, expert witnesses, Judges and court staff), candidates for tenancy, pupilage and mini pupilage can be informed of the identity and contact details of the controller, the purpose and legal basis for processing personal information and their right to withdraw consent at any time where relevant and to lodge a complaint to a supervisory body in the event of an alleged data breach.

GENERAL GUIDANCE FOR INDIVIDUAL BARRISTERS

1) All members shall maintain their registration with the Information Commissioner and notify them of any relevant changes.

2) All members shall ensure that they have adequate security measures on personal information technology (computers, laptops and smart phones) by way of a password which is either made of at least 5 letters, a number and a special character or a fingerprint

identification and that after a maximum of 10 minutes of non- use the password needs to be re entered.

3) All members shall ensure that they have an adequate antivirus anti- spyware and firewall software program on each of their devises.

4) All devises used to store information will be protected using approved encryption software which is designed to guard against the compromise of information, whole disc encryption is more satisfactory than encryption of particular folders and barristers using folder encryption alone should satisfy themselves that this will provide a reasonable level of security.

5) All confidential information should be sent and received through chambers server (emails suffixed with "PendragonChambers.com). Members should not use personal email addresses and confidential information should not be transferred to personal email addresses by any means.

4) In relation to emails the following shall apply:

a) Encryption should be used if particularly sensitive information is to be sent by email and passwords should be sent in a different email to the encrypted information

b) Use of the internet via a wireless network should be used carefully and you should never make your computer detectable by others on the network

6) When transporting confidential information the following should apply:

a) Confidential information transported in a car should be stored out of view, where practicable information should never be left in a car unattended for any time but in any event never overnight.

b) Confidential information transported on public transport should be treated in the following way:

i) Wherever possible all confidential information must be kept in close proximity to the member

ii) Where the amount of confidential information makes it impossible to keep the information in close proximity it must be kept in a secure bag within eyesight of the member.

iii) Confidential information whether in document or electronic form must not be in view of any member of the public and privacy screens should be used where possible.

7) When storing confidential information at home the following shall apply:

i) All confidential information shall be stored in a locked cupboard unless being worked on. If material is being worked on it must be kept out of the view of any other occupants/ visitors to the home

ii) Any particularly sensitive material such as police interviews or exhibits shall be kept in a locked safe

The Pupil/ Mini Pupil Undertaking

I, _____ have read a copy of the Data Protection and Information Risk Policy of Pendragon Chambers.

I agree to maintain the confidentially of all information held by Pendragon Chambers, individual members and the clerks and recognize the importance of keeping such information confidential.

I accept that in exchange for being offered a pupilage/ mini pupilage with Pendragon Chambers, I am bound by the provisions of the Data Protection and information Risk Policy of Pendragon Chambers.

I understand that I must continue to keep all information confidential even after my time with Pendragon Chambers and that this duty endures for all time

Signed:

Dated:

Signature of Practice Manager/supervising tenant BEFORE the pupilage/ mini pupilage commences the mini pupilage/ pupilage.

THE CONTRACTOR UNDERTAKING AND IDEMNITY

I, _____ have read a copy of the Data Protection and Information Risk Policy of Pendragon Chambers.

I accept that in exchange for being contracted to carry out work for Pendragon Chambers, I am bound by the provisions of the Data Protection and information Risk Policy of Pendragon Chambers.

I agree to maintain the confidentially of all information held by Pendragon Chambers, individual members and the clerks and recognize the importance of keeping such information confidential and accept that this responsibility endures for all time

I agree to indemnity Pendragon Chambers, all members and the clerks in the event that I am found to have breached my obligations to keep all information confidential and this indemnification applies to myself and or any employee/ contractor engaged by me and I accept that I am responsible for drawing the attention of any third part I engage to the provisions of this undertaking and indemnity.

Signed:

Dated:

Signature of Practice Manager/supervising tenant BEFORE the contractor/ anyone engages by them commences work

END OF POLICY DOCUMENT

PRIVACY NOTICE/ RIGHT TO OBJECT

(To be inserted in the direct access questionnaire and at the end of our terms of contract letter)

1) All clients can be informed of the identity and contact details of the controller, the purpose and legal basis for processing personal information and their right to withdraw consent at any time where relevant and to lodge a complaint to a supervisory body in the event of an alleged data breach.

2) We will use material in the course of proceedings, whether by service on opposing parties, filing in court, or otherwise

3) You have a right to object at any time to the processing of your personal data and upon receiving such an objection, we will consider the objection and notify you of the outcome without delay.

(To be inserted at the end of every email)

1) Information contained in this email is confidential to the intended recipient and may be covered by legal professional privilege. If you receive this email in error, please advice by return email before deleting it: you should not retain the email or disclose its contents to anyone.