Data Protection & Information Risk Policy

I. INTRODUCTION

Nature of document

1. This is the Data Protection and Information Risk policy for Citadel Chambers ('Chambers'), a set of barristers' chambers operating at 190 Corporation Street, Birmingham.

2. It is written to set out policy and procedure on compliance with obligations stemming from a number of sources and in particular:

   - the Data Protection Act 1998,
   - the Bar Code of Conduct,
   - the Attorney General's Guidelines on Information Security and Government Work and
   - The General Data Protection Regulation (GDPR)

   (In relation to the Attorney General's Guidelines, this document is the *Information Risk Policy* required by paragraph 2.)

3. As a matter of the GDPR regulation, Chambers is a data controller. This policy addresses its obligations as such.

4. **In addition, counsel who are members of Chambers are data controllers and have their own personal obligations as such. The fulfilment of those obligations is a matter ultimately for each member of Chambers. However, to assist them this document is written in such a way that they may adopt it as their own data protection and information risk policy. Endeavours have been made to make it suitable as such, but the responsibility to have in place proper procedures remains that of the individual member and Chambers does not assume responsibility for the fitness of this policy for individual members' needs or any breach of the law or regulatory obligations by its members.**

5. Pupils in Chambers must follow this policy and Chambers shall draw it and their obligations under the Code of Conduct to their attention

Statement of commitment

6. Chambers and its members are committed to complying with the legal and regulatory obligations on them in relation to data and confidential information and moreover committed to preserving the confidentiality of their clients' affairs.

Definitions

7. In this document the following expressions have the following meanings:

   (1) 'confidential data' refers to any data regarding a client of Chambers or a member of Chambers or their affairs or cases;

   (2) 'restricted material' refers to data categorized as such by HM Government or any government agency or other emanation of the state.

II. DIGITAL DATA

Passwords for electronic devices

8. The following requirement applies to all computers, whether laptop or desktop, all tablets, all smartphones and all other digital devices where those devices are used to record, process or otherwise work on confidential data:

   - Such devices shall be password protected and, where practicable, the password shall be of at least 9 characters, amongst these characters being examples of at least three out of four of the following species of character: upper case letters, lower case letters, numerals and symbols.

   - When unattended, whether within Chambers, at home or elsewhere, such devices shall be secured such that they cannot be accessed without entering the password.

   - Devices should be configured so that if left inactive for longer than a given period, say five minutes, they lock automatically such that they cannot be accessed without the relevant password.

Encryption of digital storage devices

9. The following requirements apply to all digital storage devices used to store confidential data including, for example, but not limited to, hard disk drives in laptop computers, hard disk drives in desktop computers and memory sticks, subject to the exceptions set out:

   - The digital storage device must be encrypted *in its entirety* using a system accredited to the FIPS 140-2 or CCTM (CESG Claims Tested Mark) standard, or to another standard generally, expertly and reasonably expected to provide a comparable level of security.

   - Encryption of a part of the device, for instance, encryption of a particular folder, is *insufficient* to meet this requirement.

10. The following exceptions apply to this requirement:

    - It does not apply to digital storage devices *sent to counsel by a client*. An example of such a device would be a Compact Disc containing data or a recording of an interview: in such circumstances there is no obligation for Chambers or counsel to encrypt the device. In such a case the rules as to security of physical data apply: see below.

- It does not apply to storage devices within any of Chambers' servers because Chambers is advised by its Information Technology contractor that such encryption would have serious implications for the performance of the Chambers network and create the potential for serious data loss. Such devices are to be protected from unauthorised access by software protecting them from remote access and by physically securing the servers.

- It does not apply to backup tapes of storage device within any of Chambers' servers. Such devices are to be protected by physically securing the backup tapes.

11. It is explicit in the above requirement that counsel taking laptops containing hard disk drives to court or to their home should only be taking digital storage devices which are securely encrypted. In this way, in the event of the loss of the hard disk drive there should be no risk that the confidential information on that drive is accessible to a third party.

Remote deletion

12. The following rule applies to mobile devices on which confidential data is stored including smartphones, tablets and laptops:

    - Where possible, the owner of the device shall seek to acquire the capability to wipe the device remotely so that in the event it is appropriated by a third party, it can be emptied of confidential data.

Backup of data

13. The following requirements apply in relation to the backup of digital storage devices on which counsel or employees of Chambers have stored confidential data:

    - All information held by Chambers – as opposed to one of its members – about a matter in which counsel is instructed shall be held centrally on the Chambers' servers' digital storage devices and these devices shall be regularly backed up and kept in a fire-proof locked container to prevent data loss.

    - All information held by counsel regarding cases shall be stored either on the Chambers' servers' digital storage devices or on other storage devices that are regularly backed up by counsel.

    - Any backup to the 'cloud' shall be done to service providers who store data according to appropriate standards of security and within the United Kingdom.

Protection against remote threats

14. The following rules relate to protecting computers from remote threats and from viruses and malware:

    - All computers used by counsel or Chambers staff shall be protected by up-to-date anti-virus and anti-spyware software, subjected to regular virus scans and protected by an appropriate firewall.

    - Bluetooth functionality on devices should be disabled when not in use.

    - The operating systems that devices utilise should be kept up to date to ensure that the latest security updates are installed.

    - Care should be exercised not to send confidential data over unsecure wireless connections.

    - Chambers shall maintain secure wireless connections and any member using wireless connections at home shall ensure they are secure ones.

Disposal of digital storage devices

15. The following requirement applies to the disposal of all digital storage devices on which information relating to Chambers' clients has been stored:

    - The device shall either be physically destroyed such that no data may be recovered from it or wiped using a method recognised as ensuring that information on the device is beyond recovery: such a method shall go beyond file deletion, single pass overwriting or formatting.

Sending of digital data

16. The following requirements apply to email communication and other methods of sending digital data.

    - Counsel and staff shall take due care to ensure that confidential information is not sent to the wrong email address.

    - Any confidential email shall include at its end a request that to the extent that it has been misaddressed, it is destroyed unread.

    - Where a client communicates using Criminal Justice Secure Mail, counsel or staff shall not forward email from that client other than by using Criminal Justice Secure Mail. All communication in relation to a matter in which the client is using Criminal Justice Secure Mail shall be by Criminal Justice Secure Mail.

    - Restricted material shall not be sent by email other than by Criminal Justice Secure Mail.

- In any case where data to be sent is of sensitivity thought shall be given (a) to whether it was appropriate to send it by non-secure email and (b) to whether if sent by non-secure email it should be sent by way of attaching an encrypted file.
- Where an encrypted file is attached to an email, the password to decode the file shall **not** be included in the email sending the file.
- Where the unintended disclosure of data to a third party would risk life, limb or national security, such data shall not be sent by email other than (a) with the client's permission, (b) in an encrypted file attached (c) to an email sent using Criminal Justice Secure Mail.

III. PHYSICAL MATERIAL

Physical security of Chambers

17. The following steps shall be taken to protect the security of Chambers:

    - When unoccupied, Chambers shall be secured by deadlocked outside doors and an armed burglar alarm and all outside windows shall be shut. Trigger of the alarm shall be monitored by a security contractor.

    - When occupied, all doors to the outside shall either be deadlocked, or locked but capable of being opened by entering a code. Codes to outside doors shall be changed regularly and not communicated to anyone who is not a member, an employee or a trusted contractor of Chambers.

    - Chambers shall maintain a system whereby it is possible for any member or member of staff leaving the building to determine whether anyone else remains in it.

Material in common parts of Chambers

18. The following rules apply to the clerks' room and other rooms in which Chambers employees work:

    - Any confidential material shall be kept in locked cabinets when the room is unoccupied.

    - When being worked on, confidential material shall not be left where someone might inadvertently read it when entering the room.

    - Counsel shall not collect faxes from the fax machine nor printing from the clerks' room printer, save in exceptional circumstances. The material shall be collected by a clerk or other responsible employee and distributed.

19. The following steps shall be taken in relation to the kitchen, library, locker room, conference rooms and any other common parts of Chambers:

    - No confidential material shall be left unattended on any desk or table.

    - Counsel must regularly check their pigeon hole and upon finding confidential material remove it for storage elsewhere: pigeon holes are to be used to effect transit of material to counsel, not to store material.

    - Any printing or photocopying of confidential data must be promptly collected and not left on the printer / photocopier.

- At regular intervals a members of Chambers staff shall examine what has been left on the locker room printer and dispose of any material which has not promptly been collected.

20. The following steps shall be taken in relation to confidential material held in counsel's rooms:

    - No one save members of Chambers, Chambers' staff, authorised contractors and those with a legal right so to do so shall enter counsel's rooms unless accompanied by a member of Chambers or a member of Chambers' staff.
    - Confidential Material shall not be left open on desks where it can be viewed by anyone going into counsel's rooms.
    - Confidential material unauthorised access to which would risk life, limb or national security shall be kept in a secure locked cabinet.

Visitors to Chambers

21. The following rules apply to visitors to Chambers:

    - Visitors awaiting attention should wait in the waiting room.
    - Visitors in other areas of Chambers should be accompanied by a member of Chambers or a member of staff at all times.
    - No visitors shall be permitted into the pigeon hole area save under constant observation.

Storage of material

22. The following rules apply to the storage of physical material:

    - Confidential data should generally be kept in Chambers, either in the relevant barrister's room or in their locker in the locker room.
    - When kept at counsel's home, confidential data should be stored in a locked cabinet.
    - Particularly confidential recordings, including recordings of interviews of complainants of sexual offences and other data that the Crown Prosecution Service puts in the same category, shall be separated and kept in one or more locked cabinets. The clerks shall keep securely the key to the cabinets and the material shall be signed in and out of the cabinet when there is need to view it. The material should not be absent from the cabinet for longer than is necessary.
    - All new furniture bought for the purposes of storing confidential papers shall be lockable.

- Copies of keys to all lockable cabinets for the storage of confidential papers shall be kept in a secure key cabinet to which clerks have access.

Transit of material

23. The following rules apply to the transit of material by post, courier, Document Exchange and fax:

    - When sending confidential data by fax, care shall be taken to ensure that it is being sent to the correct receiving telephone number and it shall be sent under cover of a sheet asking that any undelivered material be returned without its being read.

    - Where sensitive material is to be sent by post, courier or document exchange, thought shall be given to sending it by recorded or tracked delivery.

24. The following rules apply to situations in which counsel or Chambers' staff take confidential information out of Chambers:

    - When travelling by private motor car, confidential information should be stored out of sight and as inconspicuously as possible. Confidential information should not be left in a motor car unattended except where the risk of doing so is less than the risk of taking it with the person leaving the vehicle. Confidential data should never be left in a vehicle overnight.

    - Confidential data should not be left unattended on public transport. Where it is necessary on a train to have confidential data in a bag of such a size that it must be placed in the luggage rack, efforts should be made to seek to sit in sight of the luggage rack or so close to it as can be arranged. When travelling by aeroplane, where possible confidential data should be carried as hand luggage.

    - Where confidential data is such that unauthorised access to it might endanger life, limb or national security, serious thought should be given to whether steps can be taken to avoid its being taken out of Chambers. Thought should be given to whether, for instance, it would be better transported as an encrypted file on an encrypted hard disk drive than in paper form. Such data should never be left in a luggage rack on a train or hold luggage.

    - Care should be taken that the public cannot read papers or what appears on a screen when it is displaying confidential data.

Destruction of material

25. The following rules apply to the confidential material that is not returned to solicitors but instead to be destroyed:

    - Confidential material shall be destroyed by cross-cut shredding.

IV. SPECIAL RULES RELATING TO GOVERNMENT MATERIAL

Material of greater than restricted designation

26. The following rule shall be applied to material that has been designated Confidential, Secret or Top Secret by a government agency:

    - To the extent that the client requires special procedures to be followed in relation to such material, they shall be followed.

Schedule of computers used to store or work on *restricted* material

27. The following step shall be taken in relation to computers used in relation to restricted material:

    - A schedule shall be made and maintained of all computers used by counsel for storing or working on restricted material.

    - The schedule shall record the type, model and serial number of such computers together with the details and currency of any anti-virus, anti-spyware, encryption or other security software maintained on each machine.

Notification of loss of confidential material to government body

28. The following rule applies where confidential material supplied by a government body is lost:

    - In that event, the government body shall be notified of the loss of data.

V. REVIEW OF MATERIAL FOR DELETION

29. The following rules shall be followed in relation to the review of material for deletion:

- Chambers and members of Chambers shall seek not to keep confidential data longer than is necessary.
- Papers shall be returned, so far as is practicable, to the professional client as soon as is sensible.
- Chambers shall review electronic data held centrally at intervals to consider whether it can be deleted.
- Counsel shall review electronic data held at intervals to consider whether it can be deleted, provided that in so doing counsel shall have firmly in mind the possibility that appeals may proceed many years after a case is concluded and deletion of data can inhibit the just disposal of such appeals.

VI. REQUIREMENTS OF STAFF, CONTRACTORS AND MINI-PUPILS TO HANDLE MATERIAL APPROPRIATELY

30. The following rule shall apply in relation to Chambers' staff and those with whom Chambers contracts *who may have access to confidential data*:

    - Chambers shall keep a list of such persons, their contact details and their position, role or function.
    - Chambers will ensure that such persons are aware of this policy.
    - Each year Chambers shall draw to the attention of its staff and relevant contractors their obligations in relation to the confidentiality of data.
    - Chambers shall ensure that such persons are obliged to follow that policy and to maintain the confidentiality of and avoid loss of confidential data and shall arrange for contractors to sign an undertaking to the effect that they shall do so and an indemnity against any losses incurred by Chambers, any member of Chambers, any member of staff and any client of any member of Chambers, lay or professional, through their failure to comply with that undertaking.
    - All Chambers employees shall undertake to comply with the provisions of the Institute of Barristers' Clerks in relation to confidentiality.
    - Chambers shall take reasonable steps to ensure that such persons are trustworthy having regard to the confidential information to which they may have access.
    - Chambers shall subject all members of staff and those contractors who have access to Chambers in the absence of members of Chambers to a Disclosure and Barring Service check at the point they first begin their duties.

31. Chambers shall require from any mini-pupil an undertaking to keep confidential all confidential information to which they become privy during their time in Chambers and shall explain to the mini-pupil the importance of confidentiality.

VII. SPECIAL PROCEDURE WHERE MEMBERS OF CHAMBERS REPRESENT DIFFERENT PARTIES IN THE SAME CASE

32. These principles apply where members of Chambers are instructed for different parties in relation to the same matter or in other situations where different members of Chambers have different responsibilities in relation to the same case, such as where one member is counsel and another a mediator:

- Where duties of confidentiality permit, all counsel involved and all instructing solicitors (or lay clients) should be told of the situation.
- Where duties of confidentiality will not so permit, counsel instructed must ensure that Chambers is aware of the situation.
- The Senior Clerk shall consider whether it is practicable and desirable that a particular clerk deal exclusively with one party to a case and another clerk deal exclusively with another.
- Care shall be taken by all members of staff to ensure that emails and papers confidential to one party do not come into the sight or possession of counsel for another party. Where security is a particular concern, thought shall be given to providing for enhanced arrangements to guarantee confidentiality.
- Where diaries contain confidential information pertaining to counsel for one party, care shall be taken by all members of staff that counsel for other parties do not see that diary.
- Thought should be given by the Senior Clerk to suitable arrangement for the receipt of faxes.
- Thought shall be given by the Senior Clerk to ensuring that emails intended for one party do not reach the other. Emails should be sent to particular counsel's email addresses and not to general criminal, family or civil email addresses.
- Counsel on opposite sides in cases shall not discuss the case with each other save on a formal basis.
- Counsel on opposite side of cases shall exercise discretion in discussing the matter with other members of Chambers or other clerks or in such a way that they may be overheard.

VIII. REGISTRATION WITH THE INFORMATION COMMISSIONER

33. The following rules apply in relation to registration with the Information Commissioner:

- Chambers shall maintain its registration with the Information Commissioner and notify any changes in accordance with the Data Protection Act 1998.
- The members of Chambers shall maintain their registration with the Information Commissioner and notify any changes in accordance with the Data Protection Act 1998.

IX. BREACH OF CONFIDENTIALITY OF CLIENT'S AFFAIRS

34. In the event of the breach of the confidentiality of a client's affairs the following rules shall apply:

- The Senior Clerk shall ensure that all necessary steps are taken to ensure that damage arising from the breach is minimised.
- The Head of Chambers shall ensure that the barrister in question considers his position as a matter of the Code of Conduct.
- The Data Protection Officer with the Data Protection Clerk shall review its Chambers' procedures in this regard. Unless they are the barrister responsible for the breach, the Data Protection Officer shall conduct this review and report in writing, and if required orally, to the Management Committee. In the event the Data Protection Officer is the barrister responsible, the Management Committee shall oversee the review.

X. THE DATA PROTECTION OFFICER, THE DATA PROTECTION CLERK

35. The following provisions relate to the appointment of the Data Protection Officer:

- The Management Committee shall from time to time appoint a member of Chambers to the office of Data Protection Officer and in the event of a vacancy in the post the Committee shall be responsible for carrying out the functions of the Data Protection Officer until such time as that vacancy is filled.

36. The Data Protection Officer shall have the following responsibilities:

- The Data Protection Officer shall fully acquaint themselves with the provisions of the Data Protection Act 1998, the relevant provisions of the Bar Code of Conduct, the provisions of the Attorney General's Guidelines on Information Security and Government Work, the General Data Protection Regulation and other relevant provisions and guidance in relation to data protection and the obligation on counsel to preserve the confidentiality of their clients' affairs.

- The Data Protection shall digest any new regulatory provisions and guidance as it emerges.

- The Data Protection Officer shall review this policy against any new provisions or guidance and to the extent necessary propose amendments to the policy to the Management Committee.

- The Data Protection Officer shall oversee the implementation of this policy.

- The Data Protection Officer shall, once each Chambers year, report in writing and, if required, orally, to the Management Committee on the fitness of this policy and the effectiveness of its implementation.

- The Data Protection Officer shall be responsible for the keeping of the register of computers on which work is done on Restricted Material.

- The Data Protection Officer shall seek to ensure that Chambers and all members of Chambers are duly registered with the Information Commissioner.

37. The Senior Clerk shall appoint a clerk to the position of Data Protection Clerk. They shall assist the Data Protection Officer in fulfilling their duties and champion the cause of data protection amongst the staff.

ANNEX: SPECIMEN UNDERTAKING

Specimen data protection undertakings are now given.

Data Protection undertaking for mini-pupil

1. I have read the Citadel Chambers Data Protection and Information Risk Policy ('the Policy').

2. I understand the importance of maintaining the confidentiality of data held by Citadel Chambers and its members and employees.

3. In consideration of being permitted to undertake a mini-pupillage at Citadel Chambers, I undertake to maintain the confidentiality of the affairs of Citadel Chambers, its staff, its member and its lay and professional clients and I take on the obligations of confidentiality set out in the Policy as though I was a member of Chambers. These obligations shall continue for all time and not be brought to an end by the end of my mini-pupillage.

Signed: ……

Dated: …/…/……

To be completed by the proposed mini-pupil and returned to the Mini-pupillage supervisor before commencement of mini- pupillage

Data Protection undertaking and indemnity for Contractor

1. I have read the Citadel Chambers Data Protection and Information Risk Policy ('the Policy').

2. I understand the importance of maintaining the confidentiality of data held by Citadel Chambers and its members and employees.

3. I undertake to maintain the confidentiality of the affairs of Citadel Chambers, its staff, its member and its lay and professional clients, and I take on the obligations of confidentiality set out in the Policy as though I was a member of Chambers. These obligations shall continue for all time.

4. I hereby indemnify Citadel Chambers, its staff, its members and its lay and professional clients, for any losses arising from any breach of this Policy caused or occasioned by myself or any employee/contractor engaged by me.

Signed: ……

Dated: …/…/……