Essex Court Chambers
CONFIDENTIALITY PROTOCOL

1. Members of Essex Court Chambers are individual self-employed barristers who are not partners and who are personally required by Core Duty 6 and rC15.5 of the BSB Handbook to keep the affairs of each client confidential, and by rC89.5 to take reasonable steps to ensure that proper arrangements are made in Chambers to preserve such confidentiality and to manage conflicts of interest, eg where different members of Chambers act for different interests in the same case. The BSB attaches great importance to the preservation of client confidentiality.

2. In addition to their professional duties under the Code, members of Chambers potentially owe their clients directly enforceable obligations at law to preserve the confidentiality of client information.

3. Members of Chambers whose practice includes work for the U.K. Government should additionally comply with the Attorney General's Guidelines on Information Security and Government Work which can be viewed online.

4. Members of Chambers are data controllers within the scope of the Data Protection Act 1998 (COMCAS organises annual registration for members of Chambers), and must comply with their obligations under the Act. The Information Commissioner has – and exercises – power to fine data controllers who contravene the Act.

5. This Protocol sets out a number of different ways in which the administration seeks to ensure that proper arrangements are made in Chambers to preserve confidentiality, in addition to members' individual efforts and responsibilities.

6. In addition to this Protocol, members of Chambers should familiarise themselves with the Guidance which has been issued by the Bar Standards Board (https://www.barstandardsboard.org.uk/media/1666557/10__confidentiality_guidance.pdf) and by the Bar Council (http://www.barcouncil.org.uk/practice-ethics/professional-practice-and-ethics/it-issues/information-security/).

(i) Discussion of confidential matters

7. Members of Chambers should not disclose any confidential information in any (written or oral) communications with other persons unless expressly or impliedly authorised to do so.

(ii) Physical materials

8. Members of Chambers should take care to ensure that papers and other physical materials remain confidential. Within Chambers, confidential documents should not be left in a position where they may be viewed by others. Where confidential documents need to be taken outside of Chambers, members of Chambers should take care not to allow the documents to become visible to others or to members of the public. When members of the clerking team or administrative staff at Chambers handle any confidential documents, care should likewise be taken not to allow the documents to become visible to others or to members of the public.

9. Confidential documents should be printed by members on their personal printers or by Chambers' dedicated Postroom, to which members do not have access. Where a member of Chambers wishes to use the Postroom facilities, documents should be sent to a member of the clerking team or Postroom staff's password protected email addresses, with the clerk or member of the Postroom staff ensuring that those documents are printed out and then delivered to that member of chambers.

10. When confidential documents are to be returned to solicitors or disposed of, they are kept in a secure room in Chambers until this takes place. The papers should be kept in the member of Chambers' own room until they are collected and removed to the secure room. The disposal of confidential documents is carried out by security vetted waste disposal contractors.

(iii) Digital materials

11. Where Confidential data is received in a digital format, such as on a CD or memory stick, or electronic file, members of Chambers should take particular care to keep such devices safe and to ensure that their screens are not visible to members of the public when using them outside of Chambers. Members of Chambers should also ensure that information on electronic devices which they use for home working is not accessible by others. All electronic devices used for storing or accessing confidential information should be (at least) password protected, and portable devices (mobile phones, laptops, USB sticks and other memory devices) should be encrypted. Guidance is set out in the IT Committee's Memorandum of February 2015. Chambers' IT staff are available to advise and assist in protecting the security of digital information and electronic devices.

(iv) Members of Chambers involved in the same cases

12. Members of Chambers are frequently involved in the same cases, often on different sides and sometimes where one is an arbitrator and one is counsel. In such circumstances, members of Chambers and the clerking team and other administrative staff should ensure that particular care is taken to uphold client confidentiality.

13. Sometimes it will be obvious to those involved that more than one member of Chambers are involved in different teams or roles in a particular matter (such as where names appear on pleadings or following the appointment of an arbitral tribunal). When this becomes obvious or where other notification of the involvement of members of Chambers on different sides is received or where a member of Chambers is part of an arbitral tribunal on a matter in which other members of Chambers act as Counsel, a separate clerk is allocated to each member of Chambers/each such team in the case and their contact details provided to the client.

14. Each member of Chambers has a unique email account to which he or she sets a unique password to access their email account and electronic diary system. Likewise, a unique password is set for the voicemail system. No member of Chambers has access to the email account, diary, fee or case information or voicemail of any other member of Chambers.

15. If clients do not want the fact that they have taken legal advice to be known by anyone other than their advisors, this should be made clear at the outset, and it is advisable for instructions to be sent down under a project name, not including the parties' real names.

16. In any event, in respect of every case, all members of chambers should be aware that it is possible that other members of Chambers may be involved and they should always act accordingly and with due discretion.

17. Members of Chambers and the clerking team are also happy to discuss additional security measures tailored to specific client needs and concerns where necessary.

15.12.2015