Confidentiality Guidance

Maintaining confidentiality

Concern has been expressed that the profession is not taking its responsibilities to protect confidential client data and confidential financial data of members of Chambers sufficiently seriously. Examples have been given that client papers and Chambers' data are not being disposed of securely and are simply being discarded in waste paper baskets within Chambers.

The Bar Standards Board would like to remind barristers that all client communications are privileged and that such communications, client information and Chambers confidential data (financial or otherwise) must be stored, handled and disposed of securely.

Attention in particular is drawn to Core Duty 6, Rule C5 and Rule C15.5 of the BSB Handbook, which require barristers to preserve the confidentiality of the client's affairs. Any barrister who does not adhere to this by, for example, allowing other people to see confidential material, losing portable devices on which unprotected information is stored, or not disposing of client papers securely could face disciplinary action by the Bar Standards Board.

Barristers are data controllers under the Data Protection Act and must comply with the requirements of the Act in handling data to which that Act applies.

Barristers are responsible for the conduct of those who undertake work on their behalf and are advised to ensure that clerks and other Chambers' staff are aware of the need to handle and dispose of confidential material securely. Chambers must have appropriate systems for looking after confidential information.

In making arrangements to look after the information entrusted to them, barristers should seek to reduce the risk of casual or deliberate unauthorised access to it. Consideration needs to be given to information kept in electronic form as well as on paper. The arrangements should cover:

- The handling and storage of confidential information. Papers should not be left where others can read them, and computers should be placed so that they cannot be overlooked, especially when working in public places. When not being used, papers should be stored in a way which minimises the risk of unauthorised access. Computers should be password protected.
- Suitable arrangements should be made for distributing papers and sending

faxes and emails.

- Particular care should be taken when using removable devices such as laptops, removable discs, CDs, USB memory sticks and PDAs. Such devices should be used to store only information needed for immediate business purposes, not for permanent storage. Information on them should be at least password protected and preferably encrypted. Great care should be taken in looking after the devices themselves to ensure that they are not lost or stolen.
- When no longer required, all confidential material must be disposed of securely, for example by returning it to the client or professional client, shredding paper, permanently erasing information no longer required and securely disposing of any electronic devices which hold confidential information.

Additional safeguards will need to be put in place for particularly sensitive information, or for cases in which Counsel from the same Chambers are appearing on opposing sides.

January 2014
Bar Standards Board