# Confidentiality Guidance

**Maintaining confidentiality**

The Bar Standards Board (BSB) 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 their 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 BSB.

Barristers are data controllers under the Data Protection Act 2018, must comply with the requirements of the Act in handling data to which that Act applies, and must also comply with the General Data Protection Regulation (GDPR). A breach of the Act or the GDPR is likely to constitute a breach of Core Duty 10 of the BSB Handbook, which states that "you must take reasonable steps to manage your practice, or carry out your role within your practice, competently and in such a way as to achieve compliance with your *legal* and regulatory *obligations*" (emphasis added). A breach of the Act and/or the GDPR may also constitute a breach of Core Duty 5 of the BSB Handbook, which states that "you must not behave in a way which is likely to diminish the trust and confidence which the public places in you or in the profession".

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 barristers from the same chambers are appearing on opposing sides.

**Bar Standards Board**
**October 2019**