Information Security

Purpose:	To guide all barristers on good practice relating to information security
Scope of application:	All practising barristers
Issued by:	The Information Technology Panel
Last reviewed:	January 2021
Status and effect:	**Please see the notice at end of this document. This is not "guidance" for the purposes of the BSB Handbook I6.4.**

Introduction

1. The BSB Handbook (v3.5 January 2019) states:

   rC15.5 "you must protect the confidentiality of each client's affairs, except for such disclosures as are required or permitted by law or to which your client gives informed consent."
   rC89.5 "Taking into account the provisions of Rule rC90, you must take reasonable steps to ensure that proper arrangements are made [...] for [...] ensuring the confidentiality of clients' affairs;"

2. It is your individual responsibility as a barrister to preserve the confidentiality of your client's affairs. This fundamental "professional principle" has the same meaning set out in S1(3) of the Legal Services Act ("e. that the affairs of the client should be kept confidential") (BSB Handbook, Part 6 Definition 153 (p263)

3. The BSB Handbook guidance sets out at gC134 "Your duty under Rule rC89.5 to have proper arrangements in place for ensuring the confidentiality of each client's affairs includes: 1. putting in place and enforcing adequate procedures for the purpose of protecting confidential information; .2 complying with data protection obligations imposed by law; .3 taking reasonable steps to ensure that anyone who

has access to such information or data in the course of their work for you complies with these obligations; and .4 taking into account any further guidance on confidentiality which is available on the Bar Standards Board's website and which can be accessed here.

4. The General Data Protection Regulation ("GDPR") and the Data Protection Act 2018 ("DPA") contain mandatory requirements which must be complied with by barristers and sets of chambers when processing personal data. Severe penalties may be imposed in the event of non-compliance. The GDPR and the DPA together are referred to as "the Data Protection legislation".

5. In the absence of specific instructions from instructing solicitors, these guidelines are intended to apply to all material received or brought into being by barristers in connection with their professional work and which contain confidential material and/or personal data to which the Data Protection legislation applies.

6. The use of the term "should" in these guidelines refers to good practice, of application in most situations and where any deviation will require justification according to the specific circumstances; a general practice which deviates is unlikely to be acceptable. The use of the term "must" means that compliance is required to meet obligations under the BSB Handbook.

The receipt and handling of physical material

7. Confidential Material should not be left in a position where it might be read inadvertently by another person entering the room.

8. Confidential Material should not be read or worked on in public where it can be overlooked by members of the public.

9. Confidential Material should be stored in chambers or any other secure place to which the barrister instructed has regular access. If Confidential Material is removed from secure storage, you should try to restrict the amount taken out to what is necessary.

10. Confidential Material should be moved securely. On public transport Confidential Material should not be left unattended. If travelling by private car, where practicable, keep Confidential Material out of sight and store it as inconspicuously as possible. Confidential Material should not be left in a car unattended except where the risk of doing so is less than the risk of taking it with you. It should not be left in an unattended car overnight.

Material taken to Court

11. The parties' copies of court bundles and papers, and papers and copies of documents provided for the use of witnesses, i.e. not those that have previously been filed with or supplied for the exclusive use of the court (which are the responsibility of the Court), are the sole responsibility of those parties' representatives as data controllers. As data controllers, legal representatives are required to make the necessary arrangements to remove them immediately following the end of the court hearing.

12. If bundles and court papers containing sensitive, Special Category, personal data are left unattended or unsecured in the court or court building then HMCTS may consider it necessary to report that a personal data breach has occurred pursuant to the Data Protection legislation.

Physical security of electronic devices

13. You should also take appropriate steps to ensure the physical security of desktop computers, laptops, tablets, smartphones, PDAs, and USB sticks and other removable storage devices that contain Confidential Material.

14. In particular you should not:

    - leave devices in an unattended car overnight, and;

    - leave devices unattended in a public place (although there is no objection to leaving them in a locked court-room during adjournments).

15. Where possible, computers, tablets and smartphones used for professional purposes should not be placed so that their screens can be overlooked, especially in public places.

Laptops and other portable devices

16. Particular risks to client confidentiality arise from the loss of Confidential Material held on laptop computers, tablets, smartphones, PDAs, USB sticks and other removable storage devices. A single portable device may contain years of work that will contain very large amounts of Confidential Material. The loss of information that you are used to handling on a routine basis (such as previous convictions, commercial contracts, and medical reports) may cause considerable embarrassment to third parties as well as being a breach of the BSB Handbook and the Data Protection legislation. You should take as much care with this material as you would with your own valuables to prevent theft or loss.

17. You should consider restricting the amount of Confidential Material stored on portable devices to the minimum. To the extent that the Confidential Material

consists of personal data, that personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which the personal data are processed – this is the 'data minimisation' principle set out in GDPR Art. 5.1(c).

Electronic security and encryption

18. You must process personal data in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. This is the 'integrity and confidentiality' principle set out in GDPR Arts.5.1(f) and 32. You should adopt similar precautions in relation to confidential material of your clients which is not "personal data". Where appropriate, safeguards such as encryption or pseudonymisation should be adopted. Appropriate technical and organisational measures must be adopted both at the time of the determination of the means for processing and at the time of the processing itself.

19. You should use appropriate security technologies suitable for the particular device or application (for example this may include anti-virus, anti-spyware and firewall software). Regular anti-virus scans should be carried out, and the software must be kept up to date. If you are unfamiliar with the operation of such software, you should seek advice as to how to set up such scans and the updating options of software. The latest updates to the operating system software should be installed.

20. Take care to avoid infection which may result from downloading malware, for example, by clicking on links in emails or downloading attachments or programs from sources that you do not know and trust. You should be especially vigilant concerning the risk of downloading malware by visiting websites which you do not have grounds for trusting, or by clicking on links in emails or opening attachments to emails. "Phishing" emails can be fabricated to appear to have been sent by a colleague or acquaintance, so be wary of any link or attachment in an email which you were not expecting, even an email from an apparently known and trusted sender.

21. Access to computers, tablets, smartphones and other electronic devices containing Confidential Material should be protected by password:

    - You should take care to select a secure password. Passwords used to access computers or encrypted data should be sufficiently memorable that you can avoid writing them down, but not obvious or easily guessed. Long passwords are better, as a short password can be cracked more easily by

hacking software. A combination of words, using a mixture of upper case and lower-case characters and at least one numeral may be easiest to remember. Default passwords (e.g. '1234', 'admin') should always be changed. You should not use the same password for all devices, services and websites, and it is sensible to change your password from time to time and in any event if it is disclosed to another person or discovered. You should be aware that some websites store passwords in readable text. Password manager software can assist with managing and storing long complex passwords.

- Access using biometric technologies such as a fingerprint scanner or facial recognition software are acceptable alternatives.

- It is a good precaution to use two-factor authentication for websites and applications where this is available.

- Devices should be left password-protected when not in use, and should automatically log out after a period of no more than 15 minutes inactivity.

22. You should use appropriate security technologies suitable for the particular device or application (for example this may include anti-virus, anti-spyware and firewall software). It is important to ensure that the software is configured to carry out regular anti-virus scans, and the software must be kept up to date. If you are unfamiliar with the operation of such software, you should seek advice as to how to set up such scans and the updating options of software. The latest updates to the operating system software should be installed.

23. Information stored electronically should be regularly backed up, and back-up media used for Confidential Material should be locked away, if possible. Ransomware is capable of attacking back-ups stored on a back-up drive, so back-up drives should only be kept connected when backing up data. Ransomware is also capable of attacking synchronised folders, so back-up data stored in the cloud should also be recoverable from prior versions which are not stored in a synchronised folder (known as point in time recovery).

24. Computers, tablets, smartphones and other electronic devices used at home to access Confidential Material should be protected from unauthorized and unrestricted access by third parties.

25. The Information Commissioner's Office recommends that portable and mobile devices including magnetic media, used to store and transmit personal

information, the loss of which could cause damage or distress to individuals, should be protected using approved encryption software which is designed to guard against the compromise of information. Wherever practicable therefore, Confidential Material stored on laptop computers and other portable devices (such as memory sticks, CD-ROMs, removable hard disk drives, tablets, smartphones and PDAs) should be encrypted in a reasonably secure manner, or as specified by the professional client. Depending on the sensitivity of the material and the location of the device, it may also be appropriate to encrypt data stored on desktop computers. If you do not encrypt, you should be prepared to justify your position. You should recognise that there is still a risk of loss or theft of a disk or the device itself, e.g. during a break-in. Therefore, using encryption on non-mobile devices can be beneficial particularly when the physical security cannot be maintained at an appropriate level. Further guidance on encryption is available on the Information Commissioner's website, together with guidance on encryption in particular scenarios. (Encryption is necessary even on a password-protected laptop, since the password protection can easily be bypassed by removing the hard disk drive and installing it in another computer or an external disk drive holder. Password protection may also be bypassed in other ways.) The type of encryption that is appropriate will depend on the circumstances:

- Whole disk encryption is more satisfactory than encryption of particular folders.

- A computer used by family members or others may in addition require encryption of specific folders, including the user profile folder, in order to prevent unauthorized access to Confidential Material by shared users or other third parties.

- Barristers using folder encryption alone should satisfy themselves that this will provide a reasonable level of security. Some programs create temporary data files from which Confidential Material could be retrieved following loss or theft of the computer. These data files, and files containing emails, may also need to be encrypted.

- Some device providers supply full device encryption which can be enabled by the user. Check with your supplier whether this applies to your device. Although this will improve security, this encryption facility may not meet the requirements of a specific client (such as the Government).

26. It is essential to make backups of data both before and after installing encryption, since in the event of virus infection or in the event of malfunction during or after installation of the encryption program the computer may become unusable. Some defragmentation programs are incompatible with encryption programs and may

result in loss of encrypted data.

27. Appropriate software should be used for encryption. The Bar Council does not endorse any individual software program or supplier. Not all encryption software meets the guidelines for barristers undertaking government work; those guidelines can be found here.

28. Any device, code or password for the emergency recovery of encrypted material should be stored in a reasonably secure manner.Where a client expressly requires that removable devices or media provided by them are used, such device or media should be used in preference to your own, unless it is apparent that it is less secure. If it is apparent that the device or media is less secure, you should discuss this with your client, including, where necessary, your lay client.

Communication

29. E-mail is a potentially insecure method of communication. Appropriate steps, such as encryption during transmission, should be taken if it is considered necessary to send particularly sensitive information by e-mail and if required by your client. In such cases you should agree with your client what encryption to use.

30. You should never send the password required to decrypt an attachment in the same e-mail as the attachment since this would self-evidently defeat the purpose of encryption to avoid interception.

31. If you arrange for e-mails to be sent to your mobile telephone, smartphone or tablet, you should ensure that the device is suitably password-protected and, ordinarily encrypted.

32. You should take care when using the 'auto complete' function that is offered by some email systems to ensure that you do not accidentally select the incorrect email address.

33. Caution is advised when using the carbon copy (cc) function and blind carbon copy (bcc) function to ensure that you are not sending data to the incorrect recipient.

34. Lists of previously used telephone numbers, fax numbers and email addresses should be kept up to date.

35. The Data Protection legislation contains restrictions on the transfer of personal data to countries outside the European Economic Area which do not provide an adequate level of security. For this reason, reputable email service providers who

are based in and provide email storage facilities in the European Economic Area should generally be used. If you use an email service provider based elsewhere you should check that emails will be stored in a country where the law provides sufficient safeguards in relation to data protection and that terms and conditions provide sufficient assurances in relation to data security. In the case of service providers in the USA there is a known risk that emails could be accessed by governmental authorities or following a court order. Moreover, a non-US subsidiary of a US company may be required to disclose information which is stored outside the USA to US governmental authorities. You should therefore consider whether the information contained in your communications is of a nature which needs to be kept secure from US governmental authorities, such that US-owned email service providers should not be used.

36. The EU-US Privacy Shield is no longer valid for transfers of data to the USA. Standard contractual clauses ("SCC") for the transfer of personal data to processors established in third countries may still be used, provided that an adequate level of protection (equivalent to GDPR) is provided to data subjects. If necessary, additional measures (for example data minimisation, zero knowledge encryption, and pseudonymisation) must be taken to ensure this.[1]

37. Connecting to the internet via a wireless network presents a particular risk of interception of communication. You should take particular care when connecting via public and unencrypted access points. If you use a wireless network system in your home, you should ensure that it is reasonably secure.

CJSM Secure Email

38. Practitioners who use CJSM secure email, in particular, criminal defence practitioners, may find it useful to refer to the 'Frequently Asked Questions' document, which can be found here.

Cloud Computing

39. Barristers contemplating using cloud computing services, in particular services targeted at consumers generally, should assure themselves that the service provides sufficient safeguards in relation to confidentiality, security, reliability, availability and data deletion procedures. You may wish to refer to the Bar

[1] See https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/07/updated-ico-statement-on-the-judgment-of-the-european-court-of-justice-in-the-schrems-ii-case/ for the ICO's guidance on this point. The ICO guidance refers to the EDPB's FAQ at https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/07/updated-ico-statement-on-the-judgment-of-the-european-court-of-justice-in-the-schrems-ii-case/.

Council's guidance on cloud computing, the ICO's guidelines on cloud computing, and the Law Society's guidance which may also be helpful.

40. The Data Protection legislation contains restrictions on the transfer of personal data to countries outside the European Economic Area, which do not provide an adequate level of security. For this reason reputable service providers who provide storage facilities for data in the European Economic Area should generally be used. If you use a service provider based elsewhere you should check that data will only be stored in a country where the law provides sufficient safeguards in relation to data protection and that terms and conditions provide sufficient assurances in relation to data security. You should also be aware that storage facilities located outside the USA but owned by a subsidiary of a US company may be subject to US governmental surveillance. (See above in relation to transfers of data to USA.)

41. Some cloud storage facilities state that they provide encryption, but this does not mean that files stored in the cloud are accessible only to the cloud storage service provider's customer. Some cloud storage service providers are able to gain access to the contents of encrypted files in order that they can provide access in accordance with a court order or a governmental request. Barristers using cloud storage facilities to store sensitive data should consider encrypting files themselves before uploading to the cloud or using a cloud service provider whose software encrypts files before uploading.

Fax security

42. If you use fax, you should be aware of the Information Commissioner's guidelines, which are as follows:

    - Consider whether sending the information by a means other than fax is more appropriate, such as using a courier service or secure email. Make sure you only send the information that is required. For example, if a solicitor asks you to forward a statement, send only the statement specifically asked for, not all statements available on the file.

    - Make sure you double check the fax number you are using. It is best to dial from a directory of previously verified numbers.

    - So far as possible, check that you are sending a fax to a recipient with adequate security measures in place. For example, your fax should not be left uncollected in an open plan office.

- If the fax is sensitive, ask the recipient to confirm that someone is at the fax machine and ready to receive the document, and that there is sufficient paper in the machine.

- Ring up or email to make sure the whole document has been received safely.

- Use a cover sheet. This will let anyone know who the information is for and whether it is confidential or sensitive, without them having to look at the contents.

Chambers matters

43. Chambers should have an information risk policy setting out how to safeguard information in Chambers. Chambers may adopt or adapt these Guidelines or create their own policy.

44. Reasonable steps should be taken to ensure the reliability of IT and other staff who have access to IT systems. This would be likely to include checking identity and references. Encryption of particularly sensitive documents may be necessary to prevent technical staff accessing them.

45. Barristers, pupils and staff in Chambers should be given training on the importance of information security, and this training should be repeated from time to time. The ICO have training materials available on their website.

46. Chambers should have procedures in place for reporting any loss of electronic media or papers upon which or in which Confidential Material might be stored. When a loss or theft occurs, Chambers, the professional client and (if appropriate) the police should be immediately informed.

47. A log should be kept of devices upon which Confidential Material might be stored, including serial numbers, where available, and a record of encryption software installed. This will assist in the recovery of any lost or stolen items.

Outsourcing

48. Where services are outsourced and provided by third parties to Chambers, rC86 states:

> *"rC86 Where you outsource to a third party any support services that are critical to the delivery of any legal services in respect of which you are instructed:*
>
> *.1 any outsourcing does not alter your obligations to your client;*

.2 you remain responsible for compliance with your obligations under this Handbook in respect of the legal services;

.3 you must ensure that such outsourcing is subject to contractual arrangements which ensure that such third party:

.a is subject to confidentiality obligations similar to the confidentiality obligations placed on you in accordance with this Handbook;

.b complies with any other obligations set out in this Code of Conduct which may be relevant to or affected by such outsourcing;

.c processes any personal data in accordance with your instructions

.d is required to allow the Bar Standards Board or its agent to obtain information from, inspect the records (including electronic records) of, or enter the premises of such third party in relation to the outsourced activities or functions; and

.e processes any personal data in accordance with those arrangements, and for the avoidance of doubt, those arrangements are compliant with any relevant data protection laws."

49. Third parties who carry out activities on your behalf, which include processing of personal data will be data processors. You must enter into a contract with the data processor containing the matters set out in GDPR Art.28.

Disposal

50. It is a requirement of the Data Protection legislation that personal data (as defined in the Data Protection legislation) should not be retained for longer than is required. However, this may be 7 years or longer for case files. Data retention, review and deletion schedules should be set up both as part of Chambers' systems and in respect of barristers' own IT systems. These schedules should be implemented as an automatic review process by Chambers, in its capacity as a data processor in respect of data for which barristers are data controllers, as directed by barristers. Individual barristers will need to implement the schedules on their own IT systems. While some Chambers may collectively agree the same schedules, individual barristers may decide to vary these schedules to meet the requirements of their own practice. The retention of precedents, pleadings, advices and documents that have been used in open court, from which personal data have been removed by anonymising, is not a breach of the requirements of the Data Protection legislation.

51. Chambers should have procedures in place for the secure disposal of Confidential Material and electronic media (e.g. the cross-cut shredding of papers and CD-ROMs), and hard drives.

52. Barristers who wish to dispose of any computer or electronic media upon which Confidential Material has been stored must ensure the material is effectively

destroyed or wiped using a recognized method to put the data beyond recovery. Merely deleting the files, single-pass overwriting, or reformatting the disk is insufficient. Physical destruction or the use of specialist deletion and overwriting software is necessary. Further guidance on the secure disposal of hard drives is available here.

Data breaches

53. Personal data breaches, defined as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed", must be reported to the ICO, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons (see GDPR Arts. 33 and 34).

54. The report to the ICO must be made without undue delay and, where feasible, not later than 72 hours after having become aware of it. This is a short deadline, and may in particular give rise to problems at weekends.

55. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the personal data breach must also be communicated to data subjects without undue delay. This may be very time-consuming, costly and disruptive.

Other requirements and guidance

56. Barristers whose practice includes work for Government departments or agencies will need to comply with the Attorney General's Guidelines on Information Security and Government Work.

57. The Information Commissioner's website provides detailed guidance on information security. Very substantial fines may be imposed in the event of serious contravention of the Data Protection legislation. Such contraventions may include loss of laptops, portable devices or portable storage media, where the data remains accessible to third parties. BMIF have advised that such penalties are not covered by their professional indemnity insurance. Factors affecting the size of the penalty include the seriousness of the breach and the conduct of the data controller following the breach, such as when and whether or not the breach is reported to the Information Commissioner's Office. In the event that a failure to keep information secure amounts to "serious misconduct", a barrister would be obliged to report him or herself or another barrister to the Bar Standards Board under

rC65.7 or rC66 of the BSB Handbook. In the event of such a failure, a barrister is obliged to take all reasonable steps to mitigate the effects, according to the guidance (gC94) under rC65.

Important Notice

This document has been prepared by the Bar Council to assist barristers on matters of information security. **It is not "guidance" for the purposes of the BSB Handbook I6.4, and neither the BSB nor bodies regulating information security nor the Legal Ombudsman is bound by any views or advice expressed in it.** It does not comprise - and cannot be relied on as giving - legal advice. It has been prepared in good faith, but neither the Bar Council nor any of the individuals responsible for or involved in its preparation accept any responsibility or liability for anything done in reliance on it. For fuller information as to the status and effect of this document, please refer to the professional practice and ethics section of the Bar Council's website here.