Bring Your Own Device (BYOD) Policy

Purpose:	To provide a sample policy for chambers on personally-owned devices used by members of staff and pupils
Scope of application:	All barristers and chambers
Issued by:	The Information Technology Panel
Issued on:	October 2016
Last reviewed:	October 2022
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. It is not uncommon for practice managers and pupils to use personally owned computers, tablets and smartphones for purposes related to members of chambers' practices. This may be because of the cost of issuing members of staff with equipment owned by chambers, or it may be because it would be inconvenient for the practice manager or pupil to have two similar devices, one for use in connection with chambers and one for personal use.

2. Inappropriate use of personally-owned devices or unsatisfactory procedures could involve a breach of the Code of Conduct, the UK General Data Protection Regulation ("UKGDPR") and the Data Protection Act 2018. There are therefore a number of matters which should be considered by sets of chambers which allow personally-owned devices to be used for purposes related to member of chambers' practices:

   2.1. If the device is lost or stolen, confidential information might be accessible to third parties. This could lead to a fine being imposed by the ICO.

   2.2. If the member of staff ceases to be employed by chambers, or if a pupil leaves chambers, confidential information will, unless it is deleted, remain

accessible to the ex-member of staff or ex-pupil, and could be used for unauthorised purposes or disclosed to third parties (for example by a disaffected ex-employee). The continuing accessibility of this data would be contrary to the UKGDPR (for example Articles 5, 24 and 32), and could result in a fine being imposed (even if no personal data is illegitimately disclosed).

2.3. If a personally owned device is used in an insecure manner, or is used by family members, the device could be affected by malware which might thereby be transferred to the chambers network. This could cause severe disruption, even if no data is lost.

3. For these reasons and in order to comply with UKGDPR Article 24.2, sets of chambers should have a written policy which sets out the conditions under which personally-owned devices may be used by members of staff and pupils in connection with chambers' business and in connection with individual barristers' practices. Such a policy would deal with matters such as monitoring to ensure that a device is being used in a satisfactory manner, remote wiping of data in the event of loss or theft, and deletion of data in the event that the member of staff or pupil leaves chambers.

4. Pupils (unless doing their own work after their first 6 months) are data processors under UKGDPR. In order to comply with UKGDPR Article 28.3 contracts (or other binding written arrangements) are required between pupils and data controllers i.e. (a) between pupils and pupil-supervisors, and (b) between pupils and every other barrister for whom the pupil carries out work. This needs to contain each of the matters set out in Article 28.3, and can be in electronic form. The same arrangements are required for mini-pupils if they are given access to personal data.

5. A **draft** BYOD policy is set out below. It is not possible in a single draft to deal with all the varying circumstances which may apply in different sets of chambers. The draft should be regarded as a starting point which will assist sets of chambers in drafting a policy which is appropriate in their own particular circumstances.

6. The Information Commissioner has provided helpful guidance on the benefits and the risks of using company devices, bringing your own device and bringing your own software: https://ico.org.uk/for-organisations/working-from-home/bring-your-own-device-what-should-we-consider/.

[DRAFT] Policy on personally-owned devices used by members of staff [and pupils]

1. The purpose of this policy is to ensure so far as possible that personally-owned devices used by members of staff [and pupils] are used in a manner which protects client confidentiality, personal data and the confidentiality of chambers communications. This policy supplements the chambers IT policy.

2. All members of staff and pupils should be made aware, whether through IT policies or employment contracts, that chambers reserve the right to access personally-owned devices for the purpose of ensuring the effectiveness of this policy, in the event of termination of employment [or the pupillage] or if it is suspected that there has been a breach of this policy or the chambers IT policy.

3. With the approval of [ ], members of staff may use personally-owned computers, smartphones and tablet computers ("approved devices") for purposes related to chambers business.

4. [With the approval of [ ], pupils may use personally-owned computers, smartphones and tablet computers ("approved devices") for purposes related to their work.]

5. [ ] will maintain a list of approved devices setting out

   a. the type and model of each device,

   b. the date on which the device was encrypted,

   c. the name of the user of that device.

6. Approved devices must be secured by a password or a biometric access control (e.g. fingerprint scanner or facial recognition). Passwords should be sufficiently memorable that the user can avoid writing them down, but not obvious or easily guessed. Long passwords are best, as a short password can be cracked more easily by hacking software. A combination of three 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. The same password must not be used for all devices, services and websites. Passwords must be changed if a password is disclosed to another person or discovered, and in any event every six months.

7. Approved devices must be configured so that they are automatically locked after being left idle for a set time of no more than 5 minutes in the case of mobile devices and 10 minutes in the case of desktop computers.

8. Approved devices must be encrypted in a manner approved by [ ].

9. Care must be taken to avoid using approved devices in a manner which could pose a risk to confidentiality, whether by clicking on links in suspicious emails, accessing potentially harmful websites, using potentially harmful application software, using wi-fi facilities in public places (e.g. coffee shops or airports), or otherwise. Some apps may be capable of accessing sensitive information. Software which is not used should be removed from approved devices.

10. In the event that an approved device is lost or stolen, or is suspected of having been lost or stolen, [ ] must be informed as soon as possible so that such steps as may be appropriate may be taken to delete from the device the chambers email account and other data belonging to chambers or its clients, and to report the loss of the device.

11. Passwords to approved devices must be kept confidential and must not be shared with family members or third parties.

12. Approved devices must not be used by family members or other persons unless either

a. the device has been configured for separate logins to ensure restricted access to files, or

b. the member of staff [or pupil] uses the device for work using only chambers remote access.

13. Approved anti-virus software must be used on approved computers and must be kept up to date. The latest security updates to the operating system and browser software must be routinely installed on approved computers (this does not require the installation of an entirely new version of the operating system).

14. Home Wi-Fi networks must be encrypted. Caution must be exercised when using public Wi-Fi networks as public Wi-Fi networks may not be secure.

15. Approved devices must be configured to display no more than the last [ ] days of chambers emails.

16. Except in the case of an emergency, members of staff [and pupils] may not copy data from approved devices to other personally-owned devices. The data must be securely deleted when the emergency has passed.

17. Appropriate cloud storage services may be used with the permission of [ ]. Services which do not encrypt data before the data is uploaded will not be approved.

18. If an approved device needs to be repaired, appropriate steps must be taken to ensure that confidential information cannot be seen or copied by the repairer. For this reason, the arrangements for repair must be made through chambers.

19. In the event that an approved device needs to be disposed of, confidential material must be destroyed or wiped using a recognised method to put the data beyond recovery, to the satisfaction of [ ]. 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. The steps taken to delete data must be recorded in the list of approved devices, together with the date on which the steps were taken and the date on which those steps were approved by [ ].

20. In the event of a member of staff [or pupil] leaving chambers, appropriate steps must be taken to the satisfaction of [ ] to remove the chambers email account and other data belonging to chambers, Members of chambers or their clients from approved devices and cloud storage services used by that member of staff [or pupil]. The date on which those steps are taken and the date on which those steps are approved by [ ] must be recorded in the list of approved devices.

Important Notice

This document and sample policy have 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 see here.