Code	**BD.001**
Title	**Bring Your Own Device (BYOD) Policy**
Status	**Active**
Prepared by	**Stuart Hanson**
Approved by	**Andrew Buckingham**
Date Approved	**10.11.17**
Revision Number	**Version 1.0**
Date last amended	**31.10.17**
Date of next review	**31.10.19**
Contact Officer	**Stuart Hanson**
Distribution Status	**Controlled**

BRING YOUR OWN DEVICE (BYOD) POLICY

Introduction

It is not uncommon for employees, self-employed contractors and volunteers to use personally owned computers, tablets and smartphones for purposes related to work carried out by the business. This may be because of the cost of issuing members of staff with equipment owned by the business, or it may be because it would be inconvenient for the individual concerned to have two similar devices, one for use in connection with the business and one for personal use.

Inappropriate use of personally-owned devices or unsatisfactory procedures could lead to a breach of the Code of Conduct or of the Data Protection Act 1998. There are therefore a number of matters which should be considered which allow personally-owned devices to be used for purposes related to the work of the business:

a) If the device is lost or stolen, confidential information might be accessible to third parties.

b) If the member of staff ceases to be employed by the business, or if a self-employed person ceases work with the organisation or a volunteer leaves, confidential information will, unless it is deleted, remain accessible and could be used for unauthorised purposes or disclosed to third parties (for example by a disaffected ex-employee).

c) 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 business's network.

It is for these reasons why we now have a written policy which sets out the conditions under which personally-owned devices may be used by members, self-employed contractors and volunteers. The policy deals 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 someone associated with the business leaves.

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, self-employed contractors and volunteers are used in a manner which protects client confidentiality, personal data and the confidentiality of chambers communications. This policy supplements the business's IT policy.

2. All members of staff, self-employed contractors and should be made aware, whether through IT policies or employment contracts that the business reserves the right to access personally-owned devices for the purpose of ensuring the effectiveness of this policy, in the event of termination of

employment, contract or volunteering agreement or if it is suspected that there has been a breach of this policy or the business's IT policy.

3. With the approval of the senior management team, members of staff, self-employed contractors and volunteers may use personally-owned computers, smartphones and tablet computers ("approved devices") for purposes related to the business.

4. The CEO will maintain a list of approved devices

   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.

5. 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.

6. 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.

7. Approved devices must be encrypted in a way approved by the data protection officer.

8. 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, or otherwise. Some apps for smartphones and tablets may be capable of accessing sensitive information.

9. In the event that an approved device is lost or stolen, or is suspected of having been lost or stolen, the data protection officer and senior management team must be informed as soon as possible so that such steps as may be appropriate may be taken to delete from the device the business's email account and other data belonging to the business or its clients, and to report the loss of the device.

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

11. 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, self-employed contractor or volunteer uses the device for work using only remote access.

12. 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).

13. 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.

14. Approved devices must be configured to display no more than the last 7 days of the business's emails.

15. Except in the case of an emergency, members of staff, self-employed contractors and volunteers may not copy data from approved devices to other personally-owned devices. The data must be securely deleted when the emergency has passed.

16. Appropriate cloud storage services may be used with the permission of the data protection officer. Services which do not encrypt data before the data is uploaded will not be approved.

17. 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 the business.

18. 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 the data protection officer. 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 data protection officer.

19. In the event of a member of staff, self-employed contractor or volunteer leaving the business, appropriate steps must be taken to the satisfaction of data protection officer to remove the business's email account and other data belonging to the business. The date on which those steps are taken and the

date on which those steps are approved by the data protection officer must be recorded in the list of approved devices.