Chambers of John McDonnell QC

3 Stone Buildings
Lincoln's Inn
London WC2A 3XL
Tel: +44 (0)20 7242 4937
Fax: +44 (0)20 7405 3896
DX: 52 London - Chancery Lane
clerks@threestone.law
threestone.law

TEMPLATE MOBILE WORKING POLICY

1. This policy applies to my practice as a barrister and all personnel employed within the practice who remove case files, papers or other personal data from the precincts of chambers for the purposes of work.

   [Name]
   Three Stone Buildings
   Chambers of John McDonnell Q.C.
   3 Stone Buildings
   WC2A 3XL

   ICO registration no. [No]
   Bar membership no. [No]
   Bar ID No. [No]

   Date: [Date]
   Policy became operational on: [Date]
   Next review date: [Date]

Removing files

2. It is strictly prohibited to remove client files or data from chambers or my home office for any other reason than carrying out legitimate activities in connection with my practice.

3. All files, case papers or notebooks leaving the office are to be stored in an appropriately secured bag, e.g. a suitcase – which has a lock or, for smaller items, a secure folder.

4. All items used to carry case papers should have this notice clearly displayed:

   This is the property of [the barrister]. If found contact me at [INSERT MOBILE NUMBER] urgently or return to [INSERT CHAMBERS ADDRESS]. This is a secure folder, which may contain confidential information. Any interference with the material or attempts to access it is strictly prohibited.

5. Case files or papers will not be left freely available in any common area where they may be read by other individuals, e.g. in court, in robing rooms in courthouses, in coffee shops, on public transport or at home.

6. Case files will not be left in a position where another person entering the room or looking through a window might read them inadvertently.

7. Case files will not be read or worked on in public, such as on public transport or in coffee shops where they can be overlooked by members of the public, including working on phones or laptops, unless the barrister has reasonably satisfied themselves that they cannot and will not be overlooked by members of the public.

8. Case files can be worked on at home, provided that the material is put away in a locked, non-portable container when not in use. There will be appropriate physical security measures in place where any files are stored, for example the use of burglar alarms or a lock on the room the files are in.

9. All case files will be moved securely. On public transport case files will not be left unattended. If travelling by private car, where practicable, the files will be kept out of sight and stored as inconspicuously as possible. Case files will not be left in a car unattended except where doing so reduces the risk. They should not be left in a car overnight in a public place. If travelling by aeroplane, case files will be locked away in a suitcase with a lock on it, where possible kept as cabin luggage and will not be left unattended.

10. All hard copy paper disposals containing client data will meet appropriate shredding standards.

Electronic devices

11. This policy is applicable to all work and private devices which are used for professional purposes.

12. If emails from your mobile telephone, smartphone or PDA are accessed, the device will be suitably password-protected and encrypted. In addition, an ‘inbox zero’ policy will be adopted so that the number of emails stored on any device are at a minimum.

13. Computers or devices will not be placed so that their screens can be overlooked, especially when working in co-working areas or public places.

14. Extreme care will be taken to ensure that laptops, removable devices and removable storage media containing client data are not lost or stolen. In particular:

    a. such laptops and other removable devices will not be left unattended in public places.

    b. the material on any laptop or other removable device will be kept to the minimum amount necessary to enable work to be carried out efficiently.

15. The electronic storage of case files will require certain minimum levels of security.

16. All personal computers/devices used for work will be protected by up-to-date anti-virus and anti-spyware software, subjected to regular virus scans and protected by an appropriate firewall for the computer used.

17. The operating software will be checked regularly to ensure that the latest security updates are downloaded.

18. Access to all computers must be password protected.

19. All devices will be encrypted.

20. Particular care will be taken to avoid potential infection by malware, e.g. by downloading software from a source other than those which are trusted.

21. Work-in-progress will be regularly backed up, and backup media used for case files will be locked away securely.

22. Computers used for working on case files at home will be protected from unauthorised and unrestricted access by third parties, including family members. Where practicable, the ideal is a computer used only for work of the practice.

23. The use of removable storage media (such as memory sticks, CD-ROMs, removable hard disk drives and PDAs) is prohibited without the express authorisation of the barrister, and only in particular circumstances.

24. A log of all computers and devices used for storing or working on case files will be maintained. This records type, model and serial number of each device, together with the details and currency of any anti-virus, anti-spyware, encryption or other security software maintained on each machine.