RED LION CHAMBERS

18 RED LION COURT, LONDON

&

THORNWOOD HOUSE, CHELMSFORD

REMOTE WORKING POLICY

INDEX

RED LION CHAMBERS

REMOTE WORKING POLICY OF RED LION CHAMBERS

This policy applies to all members, probationary tenants, employees, agency staff, contractors, pupils and mini-pupils of Red Lion Chambers who remove case files, papers or other personal data both physical and in electronic from Chambers for the purposes of work. This policy also covers the receipt of any Chambers Post/ DX/ Courier service to a personal home address.

Removing files

It is strictly prohibited to remove client files and /or other personal data pertaining to clients, members, suppliers and employees etc. from Chambers premises without prior authorisation from authorised personnel within the organisation. Business information should not be removed from chambers premises, unless there is a clear business need to do so and should be retained only temporarily to fulfil that need.

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

2. All items used to carry personal data should have this notice clearly displayed:

This is the property of Red Lion Chambers. If found contact me at 0207 520 6000 urgently or return to Red Lion Chambers, 18 Red Lion Court London EC4A 3EB. This is a secure folder, which may contain confidential information. Any interference with the material or attempts to access it is strictly prohibited.

3. Files or papers will never be left freely available in any common area where they may be read by other individuals, e.g. in coffee shops, in court, on public transport or at home.

4. Files or papers will not be left in a position where another person entering the room or looking through a window might read them inadvertently.

5. Files or papers will never 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.

6. Files or papers 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.

7. All files and papers will be moved securely. On public transport files and papers should not be left unattended. If travelling by private car, where practicable, the files and papers will be kept out of sight and stored as inconspicuously as possible. Files and papers should not be left in a car unattended except where the risk is less of a risk than taking it with you. It should never be left in a car overnight. If travelling by aeroplane, files and papers should be locked away in a suitcase with a lock on it, where possible kept as cabin luggage and should never be left unattended.

8. Do not dispose of hard copy papers that contain any client/ employee data etc outside of Chamber's premises, including handwritten notes, Post-It notes etc. All hard copy paper disposals are to meet appropriate shredding standards in line with Chambers' retention and disposal policy.

9. Where practicable, when working remotely the printing of any documents which relate to any client, member and any employee data should be kept to a minimum. Extreme care should be taken regarding the storage of such hard copy documents and documents should be destroyed in line with Chambers' retention policy.

Electronic devices

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

1. If you access emails from your mobile telephone, smartphone or PDA, you must ensure that the device is suitably password-protected and encrypted.
2. All devices, including personal devices used for work purposes, must be subject to an IT audit carried out by Chambers or a Chambers approved IT provider.
3. In addition, you will operate an 'inbox zero' policy so that the number of emails stored on any device is at a minimum.
4. Computers or devices must not be placed so that their screens can be overlooked, especially when working in co-working areas or public places.
5. Extreme care should be taken to ensure that laptops, removable devices, and removable storage media containing client, members or employee data are not lost or stolen. In particular:
    a. such laptops and other removable devices should never be left unattended in public places or left in a car overnight.
    b. the material on any laptop or other removable device should be kept to the **minimum amount** necessary to enable work to be carried out efficiently.
6. The electronic storage of files requires certain minimum levels of security.
7. All personal computers/devices used for work must 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.
8. The operating software must be checked regularly to ensure that the latest security updates are downloaded.
9. Access to all computers must be password protected.
10. All devices must be encrypted.
11. Particular care must be taken to avoid potential infection by malware, e.g. by downloading software from a source other than those which are trusted.
12. Whilst working remotely all devices including personal devices must only be accessed via a Chambers Hosted desktop for remote a Virtual Private Network (VPN) access.
13. Computers used for working on client/ members files and any employee data, at home should 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 barrister.
14. 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 authorised personnel within chambers, and only in particular circumstances.

15. The chambers will maintain a log of all computers and devices used for storing or working on case files. This records type, model and the 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.

16. Where working remotely in a public venue such as public transport or a coffee shop, devices must not be left unattended.