**MOBILE WORKING POLICY OF:**

**GENEVIEVE SCREECHE-POWELL**

**FIELD COURT CHAMBERS**

**Policy became operational on: 19th March 2020**

**Next review date: 19 March 2021**

**Mobile Working Policy**

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/office for the purposes of work.

**Removing files**

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.

1. 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.
2. All items used to carry case papers should have this notice clearly displayed:

***This is the property of Genevieve Screeche-Powell. If found contact me at 07967 026567 urgently or return to 5 Field Court, Gray’s Inn, London, WC1R 5EF. This is a secure folder, which may contain confidential information. Any interference with the material or attempts to access it is strictly prohibited.***

1. Case files or papers will never 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.
2. Case files will not be left in a position where another person entering the room or looking through a window might read them inadvertently.
3. Case files 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.
4. 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.
5. All case files will be moved securely. On public transport case files should 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 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, case files should be locked away in a suitcase with a lock on it, where possible kept as cabin luggage and should never be left unattended.
6. Do not dispose of hard copy papers that contain any client data outside chambers, including handwritten notes, Post-It notes etc. All hard copy paper disposals are to meet appropriate shredding standards.

**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. In addition, you will operate an ‘inbox zero’ policy so that the number of emails stored on any device are at a minimum.
2. Computers or devices must not be placed so that their screens can be overlooked, especially when working in co-working areas or public places.
3. Extreme care should be taken to ensure that laptops, removable devices and removable storage media containing client data are not lost or stolen. In particular:
	1. such laptops and other removable devices should never be left unattended in public places or left in a car overnight.
	2. 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.
4. The electronic storage of case files requires certain minimum levels of security.
5. 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.
6. The operating software must be checked regularly to ensure that the latest security updates are downloaded.
7. Access to all computers must be password protected.
8. All devices must be encrypted.
9. 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.
10. Work-in-progress should be regularly backed up, and backup media used for case files should be locked away securely.
11. Computers used for working on case files 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 practice.
12. 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.