**Mobile Working Policy**

**Guidance Notes**

Use this template to reflect the security measures and standards that you adopt to securely manage, access and process data whilst working outside of your main office. We suggest that you review the document annually and update with any changes throughout the year.

Where the measures suggested below are not practicable or do not accurately reflect how you manage data remotely, you should take steps to delete and amend the policy. There may be additional security measures which you take which are not included and we would invite you to include these steps. This document should be a true reflection of your practice and should set the standards that you expect of others who may assist you with your practice, now or at a future date.

**MOBILE WORKING POLICY OF:**

**[INSERT HEALTHCARE PROFESSIONAL NAME]**

**[INSERT BUSINESS ADDRESS]**

**[INSERT ICO REGISTRATION NUMBER]**

**[INSERT DATE]**

**Policy became operational on: [1 January 2023]**

**Next review date: [1 January 2024]**

**Mobile Working Policy**

This policy applies to my practice as a [PROFESSIONAL TITLE] and all personnel employed within the practice who remove patient files, papers or other personal data from the precincts of the office for the purposes of work.

**Removing files**

It is strictly prohibited to remove patient files or data from the 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 patient files should have this notice clearly displayed:

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

1. Patient files or papers will never be left freely available in any common area where they may be read by other individuals, e.g. in waiting rooms, in clinics, in coffee shops, on public transport or at home.
2. Patient files will not be left in a position where another person entering the room or looking through a window might read them inadvertently.
3. Patient 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. Patient 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 patient files will be moved securely. On public transport patient 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. Patient 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, patient 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 patient data outside the office, 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 patient records 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 patient files should be locked away securely.
11. Computers used for working on patient 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 my practice, and only in particular circumstances.
13. I will maintain a log of all computers and devices used for storing or working on patient files. 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.

**Disclaimer: This policy template is meant to provide general guidelines only and should be used as a reference. It does not constitute legal advice. It may not take into account all relevant laws and is not a legal document. Briefed will not assume any liability that may arise from the use of this policy.**