**DATA PROTECTION AGREEMENT**

**Introduction**

This is an undertaking by **[NAME]**, an **[employee/associate/contractor]** working at **[BUSINESS NAME]**, that they will adhere to the provisions of the Data Protection Act 2018 (DPA) and the General Data Protection Regulation (GDPR).

This agreement is effective immediately and imposes a duty of confidentiality on **[NAME]**. In the event that **[NAME]**’s professional relationship with **[BUSINESS NAME]** ceases for whatever reason, the agreement to safeguard personal data and the duty of confidentiality continue indefinitely.

The **[BUSINESS NAME]**’s privacy policy can be found on the business website **[PAGE URL]** and describes how personal data may be used.

**Processing of Personal Data**

I agree that all records containing patient personal data, whether paper or electronic, remain the exclusive property of **[BUSINESS NAME]**. I also understand that patients’ medical information constitutes “Special Category Data” as defined by the GDPR and must be accorded even greater protection than other data.

I agree that I will only process patient information in accordance with the provisions of the DPA and GDPR. To that end I understand that I may access, process, store or share patients’ data only to the extent necessary to fulfil my role within **[BUSINESS NAME]**, and provided it is within the terms of the business’s privacy policy. Any activity relating to personal data of patients or other staff members may take place only in accordance with written instructions from **[BUSINESS NAME]**.

I agree that I will not provide access to personal data by any other person or agency without the prior consent of **[BUSINESS NAME]** and under a written contract.

I will assist **[BUSINESS NAME]** where necessaryin ensuring that data subjects (patients and staff) are able to exercise their rights under the GDPR, including requesting access to their records.

I will assist **[BUSINESS NAME]** in meeting its GDPR obligations in relation to the security of personal data. In particular I will:

* notify **[BUSINESS NAME]** of personal data breaches as soon as I become aware of them
* take all appropriate measures to ensure the security of data processing
* assist with data protection impact assessments, where appropriate
* not disclose computer passwords, and will ensure that computers I am using are not left unattended unless the screen is locked
* lock all record cabinets which I am using unless I or another authorised person is monitoring their security
* not leave keys to cabinets containing personal data unattended, nor will I have copies of such keys made, without the expressed permission of management
* not share any personal data which comes to me as a result of my relationship with **[BUSINESS NAME]** with any other person or agencywithout authorisation from the Data Controller
* Do my best to prevent personal data records from unlawful access or destruction.

I will delete or return all personal data to **[BUSINESS NAME]** as requested when my professional relationship with the business ceases.

In order to meet the Article 28 obligations of the GDPR, I agree to submit to audits and inspections should they be required, and will provide **[BUSINESS NAME]** with whatever information it needs to ensure that we are both compliant with the GDPR.

I will inform **[BUSINESS NAME]** immediately if I am asked to do something infringing the GDPR or other data protection law of the EU or a member state.

I have read this data protection agreement and confirm, my agreement. I also confirm that I will uphold the highest standards in protecting patients records from unlawful access or destruction.

Name: ……………………………………………… Signature: …………………………………………….. Date: …………………………..……………