**Dr Nagpals Surgery**

**PRACTICE STAFF CONFIDENTIALITY AGREEMENT**

***Including Data Protection and Information Security***

You may not during the course of your employment with the Practice or after the termination of your employment disclose to anyone other than in the proper course of your employment or where required by law, any information of a confidential nature relating to the Practice or its Business or Patients.

You may have access to, see or hear, confidential information concerning the medical or personal affairs of patients, staff or associated healthcare professionals and unless you are acting on the instructions of an authorised officer within the Practice, on no account should such information be accessed, divulged or discussed except in the performance of your normal duties. Breach of confidence, including the improper passing of confidential data, could result in disciplinary or legal action.

Without limiting the generality of the above, for the purpose of this clause, “confidential information” covers any information relating to the Practice, its business, and activities including, but not limited to, person and patient identifiable information and other sensitive information in whatever form. It also includes all other information provided to you which is either labelled or expressed to be confidential or given to you in circumstances where one would expect the information to be confidential to the Practice.

However, it excludes any matter that has already become public knowledge or part of public record.

You should also be aware that regardless of any action taken by the Practice, a breach of confidence could result in a civil action against you for damages.

**By signing this Agreement, you undertake:**

* To treat as confidential all information that may be derived from, or be obtained during, the course of your employment with the Practice and thereafter.
* To only access areas of the Practice where confidential information is held if permissions are granted.
* To respect the rights of patients to confidentiality and privacy. This includes all persons other than the patient, as patients may not wish others (i.e. their friends/relatives) to know that they have had tests, been prescribed medication, or even visited the Practice.

**Individuals who have permission to access the Practice’s clinical system/confidential information must:**

* Acquire an individual Username and Password in order to carry out work activities electronically (enabling the Practice to conduct audit trails, if and when required).
* Log in using their designated Smartcard only and use it in accordance with the Practice’s Smartcard Usage Policy.
* Only carry out the work activities they have permission to perform (in-line with their work role).
* Consult with the Information Governance Lead/Caldicott Guardian in the event of data needing to be transferred electronically (via a secure method i.e. nhs.net, encrypted memory stick).
* Comply with the Data Protection Act 2018 which states that personal data should be:

“(a) processed lawfully, fairly and in a transparent manner in relation to individuals (‘lawfulness, fairness and transparency’);

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes (‘purpose limitation’);

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’);

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals (‘storage limitation’);

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’).”

* Ensure that all records, including computer screens, printouts, hospital letters, patient notes, faxes, etc. are never left in such a manner that unauthorised persons can obtain access to them.
* Ensure that they log out of the computer system on completion of electronic work activity, removing and safeguarding their Smartcard and log in details.
* Adopt a clear desk policy thus ensuring that confidential information is kept secure at all times

Any security breaches will be reported to the IG Lead or Caldicott Guardian of the Practice

Should any serious untoward incident occur, this will be escalated to the commissioning organisation for appropriate action/investigation.

I have read, understood and agree to comply with the Practice’s Staff Confidentiality Agreement which will be read in conjunction with the Staff Confidentiality Code of Conduct. The Practice’s Staff Confidentiality Agreement will be reviewed on an annual basis and a new Agreement will be signed to supersede this Agreement where changes are required to comply with developments in legislation or procedures.

|  |  |
| --- | --- |
| **Name** |  |
| **Job Title** |  |
| **Name of Line Manager** |  |
| **Employee Signature** |  |
| **Date** |  |