**DATA PROTECTION POLICY**

**INTRODUCTION**

The Data Protection Act 1998 (DPA) & GDPR (2018) requires a clear direction on policy for security of information within the practice. The policy will provide direction on security against unauthorised access, unlawful processing, and loss or destruction of personal information. The following is a Statement of Policy which will apply.

**THE POLICY**

* The practice is committed to security of patient and staff records.
* The practice will display a poster in the waiting room explaining to patients the practice policy on how the GDPR affect their rights (The text of the poster is below in RED)
* The practice will make available a brochure on Access to Medical Records and Data Protection for the information of patients.
* The practice will take steps to ensure that individual patient information is not deliberately or accidentally released or (by default) made available or accessible to a third party without the patient’s consent, unless otherwise legally compliant. This will include training on Confidentiality issues, DPA principles, working security procedures, and the application of Best practice in the workplace.
* The practice will undertake prudence in the use of, and testing of, arrangements for the backup and recovery of data in the event of an adverse event.
* The practice will maintain a system of “Significant Event Reporting” through a no-blame culture to capture and address incidents which threaten compliance.
* DPA issues will form part of the practice general procedures for the management of risk.
* Specific instructions will be documented within confidentiality and security instructions and will be promoted to all staff.

GENERAL DATA PROTECTION REGULATION (GDPR)
GDPR - WHAT WILL IT MEAN FOR PATIENTS

The General Data Protection Regulation (GDPR) is a new law that determines how your personal data is processed and kept safe, and the legal rights that you have in relation to your own data. The regulation applies from May 25 2018 and will apply even after the UK leaves the EU.

The GDPR sets out key principles about processing data, for staff or patients;

* Data must be processed lawfully, fairly and transparently
* It must be collected for specific, explicit and legitimate purposes
* It must be limited to what is necessary for the purposes for which it is processed
* Information must be accurate and kept up to date
* Data must be held securely
* It can only be retained for as long as is necessary for the reasons it was collected
* Being informed about how their data is used
* Patients to have access to their own data
* Patients can ask to have incorrect information changed
* Restrict how their data is used
* Move their patient data from one health organisation to another
* The right to object to their patient information being processed (in certain circumstances)