Introduction

The General Data Protection Regulations 2018 (GDPR) requires a clear direction on Policy for security of information within the Practice.

The policy provides 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 the practice policy to patients.
- 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.

Signed:

....

Caldicott Guardian Practice Manager

Date: 15.6.2018 Date: 15/6/18