EVERSLEY MEDICAL CENTRE

Information Security Policy

1. Introduction

This information security policy shall apply to information, systems, networks, applications, locations and staff of the Practice. It is based on the expectations set out within the Information Security Management: Code of Practice for NHS organisations https://www.gov.uk/government/publications/information-security-management-nhs-code-of-practice

2. Purpose

The purpose of this policy is to enable and maintain effective security and confidentiality of information processed or stored by the federation. This shall be achieved by:

- Ensuring that all members of staff are aware of and shall comply with relevant legislation, including the Data Protection Act 2018
- Describing the principles of information security management and describing how they shall be implemented within the practice
- Introducing an approach to information security that is consistent with other NHS organisations
- Assisting staff to identify and implement information security as an integral part of their day to day role
- Safeguarding information relating to staff and patients part of the practice

3. Objectives

Key objectives of the Practice's Information Security Policy are to preserve:

- Confidentiality – Access to information shall be restricted to those GPs and staff of the Practice with agreed authority to view it

- Integrity – Records are to be complete and accurate with all filling and management systems operating correctly

- Availability – Information shall be readily available and delivered to the authorised GP, medical, or other healthcare professional when it is needed

4. Responsibilities

Responsibility for information security shall rest with the Senior Partners with lead responsibility for information governance. However, on a day to day basis the Practice Manager shall be responsible for organising, implementing and managing this policy and its related good working practices.

5. The Practice shall undertake to ensure:

- Contracts of employment – Address information security requirements at the recruitment stage.

- Access controls – To areas containing information systems are restricted and controlled to ensure that only GPs, medical and other health professionals and those authorised can access information of the Practice.

- Equipment security – Is effective in order to minimise losses, or damage to the Practice. All information assets and equipment shall, where possible be physically protected from security threats and environmental hazards.

- Information risk assessment – A regular assessment of the working environment shall be conducted to identify potential risks to security of practice information.

- Protection from malicious software- should be provided through the use of commercial strength anti-virus/anti-malware software. Where there is an internet connection an appropriate firewall shall be installed and managed. No new software shall be downloaded or installed on computer systems of the Practice without the explicit permission of the Practice Manager. Breach of this requirement may be subject to disciplinary action.

- Business continuity plans and disaster recovery plans – Are in place so that in the event of a disruption to the information services for the Practice, it is possible to activate relevant business contingency plans until affected services are restored.

Signed : *Dawn Van Cooten*
Name : Dawn Van Cooten
Date:
Review Date: February 2021