CATHAYS SURGERY
DATA PROTECTION POLICY

INTRODUCTION

The General Data Protection Regulations May 2018 (GDPR) requires a clear direction on policy for security of information within the practice and provides individuals with a right of access to a copy of information held about them.

The practice needs to collect personal information about people with whom it deals in order to carry out its business and provide its services. Such people include patients, employees (present, past and prospective), suppliers and other business contacts. The information we hold will include personal, sensitive and corporate information. In addition, we may occasionally be required to collect and use certain types of such personal information to comply with the requirements of the law. No matter how it is collected, recorded and used (e.g. on a computer or on paper) this personal information must be dealt with properly to ensure compliance with the **General Data Protection Regulations Act May 2018.**

The lawful and proper treatment of personal information by the practice is extremely important to the success of our business and in order to maintain the confidence of our service users and employees. We ensure that the practice treats personal information lawfully and correctly.

This policy provides direction on security against unauthorised access, unlawful processing, and loss or destruction of personal information.

Our Access to Medical Records policy* covers Subject Access Requests under the Data Protection Act.

1.0 General Data Protection Regulation Principles

The GDPR sets out seven key principles:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

These principles should lie at the heart of your approach to processing personal data.

2.0 Employee Responsibilities

All employees will, through appropriate training and responsible management:

- comply at all times with the above GDPR principles
- observe all forms of guidance, codes of practice and procedures about the collection and use of personal information
- understand fully the purposes for which the practice uses personal information
- collect and process appropriate information, and only in accordance with the purposes for which it is to be used by the practice to meet its service needs or legal requirements
- ensure the information is correctly input into the practice's systems
- ensure the information is destroyed (in accordance with the provisions of the Act) when it is no longer required
- on receipt of a request from an individual for information held about them by or on behalf of immediately notify the practice manager
- not send any personal information outside of the United Kingdom without the authority of the Caldicott Guardian / IG Lead.
- understand that breaches of this Policy may result in disciplinary action, including dismissal

3.0 Practice Responsibilities

The practice will:

- Ensure that there is always one person with overall responsibility for GDPR. Currently this person is the Practice Manager, should you have any questions
- Maintain its registration with the Information Commissioner's Office
- Ensure that all subject access requests are dealt with as per our Subject Access to Medical Records policy
- Provide training for all staff members who handle personal information
- Provide clear lines of report and supervision for compliance with GDPR
- Carry out regular checks to monitor and assess new processing of personal data and to ensure the practice's notification to the Information Commissioner is updated to take account of any changes in processing of personal data

- Develop and maintain GDPR procedures to include: roles and responsibilities, notification, subject access requests, training and compliance testing

- Display a poster in the waiting room explaining to patients the practice policy (see below)

- Make available the practice policy on “How we use your information” patients.

- 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, GDPR principles, working security procedures, and the application of best practice in the workplace.

- Maintain a system of “Significant Event Reporting” through a no-blame culture to capture and address incidents which threaten compliance.

- Ensure confidentiality clauses are included in all contracts of employment.

- Ensure that all aspects of confidentiality and information security are promoted to all staff.

- Remain committed to the security of patient and staff records.