Data Protection Policy

1. Introduction

Information is central to everything we do in Practice; from the clinical management of individual patient health, to the efficient management of services and resources. It plays a pivotal role in the management of performance, service planning and clinical governance.

It is, therefore, crucial to ensure that information is efficiently managed and that appropriate procedures, policies and accountabilities are implemented to provide a robust framework for the management of information we gather, generate and store.

2. Definitions

Data Subject(s) – a person (people) who have information about them stored
Current and former employees; workers; volunteers; consultants; apprentices; patients

Data Controller – a person or company who gathers personal data about an individual(s)
The Practice is a Data Controller for the Data Subjects identified above

Personal Data – information relating to a data subject that can be used to identify them on its own **or** in combination with other information likely to be collected by the practice
Date of Birth, Address etc

3. Data Protection Legislation

The General Data Protection Regulations 2017 (GDPR) prompted a review of the Data Protection Act 1998 (DPA 1998) in the United Kingdom to reflect the changes in modern-day society that affects how individuals and businesses collect and use information they obtain during normal business activities.

The Data Protection Act 2018 (DPA) incorporated the changes that GDPR introduced and embedded them in British law.

4. Data Protection Principles

The practice supports and complies with the six principles of the DPA (shown below):

a. The processing of personal data must be lawful, fair and transparent
b. Personal data collected must be used for a specific and explicit purpose
c. Data collected must be adequate, relative and not excessive for the purpose
d. Data is accurate, kept up-to-date and that inaccurate or out of date information is rectified or destroyed without delay
e. Personal data must not be kept longer than necessary for the purpose for which it was gathered
f. Personal data must be processed in a manner that ensures appropriate security measure are taken

5. Purpose

The Practice needs to collect personal data about people with whom it deals in order to carry out its business and provide an effective service.
Such people include patients, employees (past, present & prospective), suppliers and other business contacts.
The information we gather will include personal, sensitive and corporate information to comply with the requirements of the law. The information we process may be:

- information supplied directly to us by the Data Subject
- information supplied by another medical professional
- information supplied by another organisation:
  (This may be information supplied by a support worker, the police or other public authority, for example)
- Information generated during the course of our normal activities (medical information)

No matter how this information is collected, used and recorded (digitally or manually), this information will be dealt with properly according to compliance with the relevant legislation.

6. Practice Responsibilities

The practice will:

a. Ensure that there is always one person with overall responsibility for data protection. Currently this person is **Dr Craig Kyte**. Responsibility will pass to **Sue Bramley** and **Craig Stocker** if the first named person is absent for any reason.
b. Maintain its registration with the Information Commissioner's Office.
c. Ensure that all Subject Access Requests (SARs) are dealt with according to the policy
d. Provide training for all employees who handle personal information
e. Provide clear lines of report and supervision for compliance with data protection and have a system for reporting breaches
f. Carry out regular checks to monitor and assess new processing of personal data and ensure the practice's notification to the Information Commissioner is updated to take into account any changes in processing of personal data
g. Develop and maintain DPA procedures to include: Roles and responsibilities; notification; subject access; training and compliance testing
h. Display a poster in reception explaining the practice policy & the Information Commissioner's certificate
i. Make available a leaflet or poster in reception on Subject Access Requests for the information of patients
j. Take steps to ensure that individual patient information is not deliberately or accidentally released or made available or accessible to a third party without the patient's consent, unless otherwise legally compliant. This will include employee training on confidentiality issues, DPA principles, security procedures and the application of best practice in the workplace.
k. Undertake testing of the arrangements for the backup and recovery or data to simulate an adverse event
l. Maintain a system for Significant Event Reporting and promote a no-blame culture to ensure events that threaten compliance are captured and learning outcomes implemented
m. Include DPA issues as part of the Practice's general procedures for risk management
n. Ensure confidentiality clauses are included in all employment contracts
o. Ensure that all aspects of confidentiality and information security are promoted to all employees
p. Remain committed to the security of all records
q. Ensure that any personal staff data requested by the CCG or NHS is not released without the written consent of the staff member.

7. Employee Responsibilities

All employees will, through appropriate training and responsible management:

a. Comply at all times with the Principles of the DPA
b. Observe all forms of guidance, codes of practice and procedures about the collection and use of personal information
c. Understand the purposes for which the practice uses personal information
d. Collect and process appropriate information – only in accordance with the purposes for which it is to be used by the practice to meet its service needs or legal requirements
e. Ensure the information is correctly input into the practice's systems
f. Ensure that information is destroyed in accordance with the DPA when it is no longer needed.
g. On receipt of a request from an individual for information held about them, or on behalf of someone else, immediately pass the request to the appropriate person
h. Not send any personal information outside of the United Kingdom without the authority of the Caldicott Guardian / IG Lead
i. Understand that breaches of this policy may result in disciplinary action, including dismissal.

8. Relevant Policies / SOPs

- Information Governance Policy
- Access to a Deceased Patient's Medical Records Policy

- Caldicott Guardian Policy
- Computer and Data Security Policy
- Internet and Email Acceptable Use Policy
- Freedom of Information Policy
- Confidentiality Policy
- Confidentiality (Dispensers) Policy
- Records Retention Policy
- Subject Access Request Policy
- Subject Access Request Standard Operating Procedure

These policies will be reviewed on an annual basis.

References

The Data Protection Act (2018)
http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

"About the DPA 2018" – Information Commissioner's Office
https://ico.org.uk/for-organisations/guide-to-data-protection/introduction-to-data-protection/about-the-dpa-2018/

9. Policy Review

This policy will be reviewed annually, or in response to a significant event or legislative change.

Version	Revisions	Due for Review	Date Reviewed
1.2	References made to the DPA 2018 (previously annotated as Data Protection Bill) and its Principles. Practice and Employee responsibilities highlighted for clarity. Section 5 added to reference the Practices explicit purpose as a data controller Section 8 added to reference linked policies / procedures	~~30th January 2021~~	25th January 2021
1.3	Updated contact names in Section 6.a	~~24th January 2022~~	9th April 2021
1.4	Added review definition to section 9	~~8th April 2022~~	13th June 2022
1.5	No changes	~~12th June 2023~~	12th May 2023
1.6	No changes	11th May 2024	

Reviewed by: Craig Stocker – Quality Assurance Manager