DATA PROTECTION POLICY

VERSION NUMBER	v.1.2
AUTHOR/LEAD	Alison Shelton
Implementation Date	September 2015
Date of last review	October 2018
Date for next formal review	October 2019
Date of Authorisation	26/05/15

VERSION	DESCRIPTION OF CHANGE	REASON FOR CHANGE	AUTHOR	DATE
v.1.0	New Policy		AS	26.05.15
v.1.0	No change		AS	15.11.16
v.1.0	No change		BM	06.11.17
v.1.1	Updated	New GDPR/DPA	SS	17.10.18
v.1.2	Updated	DSPToolkit	SS	07/11/18

Introduction

GDPR and the Data Protection Act 2018 (DPA) 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 GDPR and the **Data Protection Act 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.

This policy shall apply to partners and employees of the practice and any other person or organisation required to process personal data on our behalf.

1.0 Data Management

The recording of data within the practice is under the management and control of Alison Shelton, Managing Partner, who is the IT lead for the practice.

The quality of data, the use of templates and the use of specific coding is reviewed on an ongoing basis and the findings are discussed at clinical policy meetings, where examples of coding issues are cited as appropriate.

Alison Shelton is responsible for overall coding and data quality issues within the practice and will ensure accuracy and consistency in coding among both the clinicians and the administrative or casual staff.

Alison Shelton is also the non-clinical manager responsible for audit and exception identification and reporting within the practice.

This responsibility is supported by frequent audit and validation of data using QOF and other tools, and is also supported by a data administrator employed for this purpose.

It is the responsibility of the practice manager/ administrator/ summariser to distribute updates read codes as and when they become available.

Any Staff queries regarding the accuracy of any data shall bring this to the attention of Alison Shelton her deputy or the lead GP as soon as possible so the correct guidance can be given.

2.0 Data Protection Principles

We support fully and comply with the eight principles of the Act which are summarised below: Any person processing personal data must comply with the eight enforceable principles of good practice and observe any instructions issued in relation to the processing of personal data.

1 Personal data shall be processed fairly and lawfully.

2 Personal data shall be obtained/processed for specific lawful purposes.

3 Personal data held must be adequate, relevant and not excessive.

4 Personal data must be accurate and kept up to date.

5 Personal data shall not be kept for longer than necessary.

6 Personal data shall be processed in accordance with rights of data subjects.

7 Personal data must be kept secure.

8 Personal data shall not be transferred outside the European Economic Area (EEA) unless there is adequate protection.

<u>Fair and lawful processing</u>

The Data Protection Act is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject. The data subject must be told who the data controller is, who the data controller's representative is, the purpose for which the data is to be processed by us, and the identities of anyone to whom the data may be disclosed or transferred.

For personal data to be processed lawfully, certain conditions have to be met. These may include, among other things, requirements that the data subject has consented to the processing, or that the processing is necessary for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed,

more than one condition must be met. In most cases the data subject's explicit consent to the processing of such data will be required.

Limited purpose and appropriateness

Personal data may only be processed for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by the Act. This means that personal data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed of the new purpose before any processing occurs.

Adequate, relevant and non-excessive processing

Personal data should only be collected to the extent that it is required for the specific purpose notified to the data subject. Any data that is not necessary for that purpose should not be collected in the first place.

Accurate data

Personal data must be accurate and kept up to date. Information that is incorrect or misleading is not accurate and steps should therefore be taken to check the accuracy of personal data at the point of collection and at regular intervals thereafter. Inaccurate or out-of-date data should be destroyed.

Timely processing

Personal data should not be kept longer than is necessary for the purpose. This means that data should be destroyed or erased from our systems when it is no longer required. Guidance on how long certain data is to be kept before being destroyed will be given in the Records Retention Policy

Processing in line with the data subject's rights

Data must be processed in line with data subjects' rights. Data subjects have a right to:

request access to any data held about them by a data controller;

prevent the processing of their data for direct-marketing purposes;

ask to have inaccurate data amended; or,

prevent processing that is likely to cause damage or distress to themselves or anyone else.

Data security

We must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. Data subjects may apply to the courts for compensation if they have suffered damage from such a loss. Also, our reputation relies on managing data protection effectively to avoid potential adverse publicity and reputation damage from any failure.

The Act requires us to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third party's data processor if they give explicit agreement to comply with those procedures and policies, or if they put in place adequate measures themselves. Whenever practicable data pseudonymisation should be utilised, unless this would frustrate the purpose of the data sharing.

Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

Confidentiality means that only people who are authorised to use the data can access it.

Integrity means that personal data should be accurate and suitable for the purpose for which it is processed.

Availability means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should not normally, therefore, be stored solely on our individual PCs.

Security protocols include:

Entry controls: Entry and movement around the premises must be strictly controlled through appropriate authorisation and unauthorised persons seen in entry-controlled areas should be reported.

Secure, lockable desks and cupboards: Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)

Methods of disposal: Paper documents should be shredded or securely disposed of through approved means. Digital/optical media should be physically destroyed when they are no longer required.

Equipment: Data users should ensure that individual monitors do not show confidential information to passers-by and that they lock/log off from their PC when it is left unattended.

3.0 Employee Responsibilities

All employees will, through appropriate training and responsible management:

- comply at all times with the above Data Protection Act 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 securely 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 managing partner Alison Shelton

- 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

4.0 Practice Responsibilities

The practice will:

- Ensure that there is always one person with overall responsibility for data protection. Currently this person is Alison Shelton, should you have any questions about data protection

- Maintain its registration with the Information Commissioner's Office

- Ensure that all subject access requests are dealt with as per our 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 data protection

- Carry out a Data Protection Impact Assessment (DPIA) to 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 taking into consideration the principles of Data Protection by design and default.

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

- Display a poster in the waiting rooms explaining to patients the Practice Privacy policy.

- Make available a brochure on Access to Medical Records for the information of 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, DPA principles, working security procedures, and the application of best practice in the workplace.

- Undertake prudence in the use of, and testing of, arrangements for the backup and recovery of data in the event of an adverse event.

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

- Maintain a register of data breaches and action taken.

- Undergo periodic spot check audits of data security at least every 6 months.
- Include DPA issues as part of the practice general procedures for the management of risk.
- 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.

Signed:	Signed
Information Governance Lead	Practice Manager
Date:	Date: