Date published: **June 2022**
Review Date **June 2023**

WESTOVER SURGERY

DATA PROTECTION POLICY

Brief summary of document: This Policy outlines how the Practice will meet its legal obligations and NHS requirements, concerning confidentiality and information security standards. The requirements within the Policy are primarily based upon the Data Protection Act 2018 (The Act); including GDPR the key piece of legislation covering security and confidentiality of personal information.

1 Introduction

Westover Surgery is bound by the provisions of a considerable number of items of legislation and regulation affecting the control of person identifiable data.

Westover Surgery Overarching Information Governance Policy defines the Practice's mandated approach for compliance and effective management in each of the following five areas of Information Governance.

- Openness
- Legal Compliance
- Information Security
- Quality assurance
- Records Management

Each of these five areas has detailed policies and associated procedures which collectively constitute the top level documentation of the Practice's Information Governance Management.

2 Purpose

This Policy outlines how the Practice will meet its legal obligations and NHS requirements, concerning confidentiality and information security standards. The requirements within this Policy are primarily based upon the Data Protection Act 2018 (The Act); the key piece of legislation covering security and confidentiality of personal information. A brief summary of the Act and associated legislation and policies and principles are detailed below.

3 Scope

This Policy applies to Person identifiable data (staff, service user and other data subject information) that is either held or processed by the Practice.

4 Roles and Responsibilities

The Clinical Governance Partner Lead Is the Accountable Officer for the Practice has overall accountability for Information Governance in the Practice, and is required to provide assurance, through the Statement of Internal Control (SIC), that all risks relating to information are effectively managed, and also acts as Practice Caldicott Guardian, who is responsible for championing the principles of Data Protection and Confidentiality within the Practice.

The Information Governance and Technology Security Manager is responsible for the availability and review of this policy and associated procedures, and is responsible for achieving compliance with NHS and legal standards of information technology security.

The Clinical Governance Lead is responsible for the review and maintenance of this policy co-ordinating the administration of subject access requests, maintenance of the database register and dealing with general day to day data protection queries.

All Staff

All Practice staff and those working on behalf of the Practice in any capacity that work with/have access to person identifiable data are required to adhere to this policy and to follow the associated procedures where appropriate.

Expert Advice

Expert advice in support of this policy will be provided by the Manager of Information Governance Protection and the Caldicott Guardian.

5 Policy Statement

All Person identifiable data held or processed by the Practice, as the Data Controller, will be held and processed in accordance with the requirements of the Data Protection Act 1998 (the Act).
There are eight principles of good practice within the Data Protection Act 1998.

6 The Data Protection Principles

Principle 1

Person identifiable data shall be processed fairly and lawfully

There is a requirement to make the general public aware, who may use the services of the NHS, of why the NHS needs information about them, how this is used and to whom it may be disclosed or shared with. The Practice is obliged under the Data Protection Act and Caldicott principles to produce patient information leaflets and posters for public information.

The NHS complies with the Data Protection Act requirements and also an individual's right to privacy under the 1998 Human Rights Act.

Principle 2

Person identifiable data shall be obtained for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

All databases that hold and/or process personal information about living individuals must be registered. A nominated person will be responsible as a database controller for each registered database. A log of databases and nominated controllers will be maintained by the Data Protection Officer.

A database is any collection of personal information that can be processed by automated means.
A few examples are detailed below:
· Patient records (names and addresses etc.) for appointments;
· Patient details used for prescribing drugs;
· Patient information used for research e.g. where only NHS number (or other personal identifier may be allocated) and clinical details may be held – this could be an Excel spreadsheet;
· Staff records held on Excel to monitor annual leave and sickness.

Principle 3

Person identifiable data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

Information collected from individuals should be complete and should all be justified as being required for the purpose they are being requested.

Principle 4

Person identifiable data shall be accurate and, where necessary, kept up to date

Accuracy/data quality – the Practice will ensure that all information held on any media is accurate and up to date. The accuracy of the information can be achieved by implementing validation routines, some of which will be system specific and details must be provided of these validation processes to the system/information users. Users of software are responsible for the quality (i.e. accuracy, timeliness, completeness) of their data by carrying out their own quality assurance and participating as required in quality assurance processes.

Staff should check with patients that the information held by the Practice is kept up to date by asking patients attending appointments to validate the information held.

Staff information should also be checked for accuracy on a regular basis by the Practice Manager.

Principle 5

Person identifiable data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes

This principle applies to all records regardless of the media on which they may be held, stored or retained. Further details of how this affects the Practice, and actions required to comply with it, are detailed in the Practice Records Management Policy.

Principle 6

Person identifiable data shall be processed in accordance with the rights of data subjects under this Act

Individual's rights – include subject access and right to complain

Under this principle of the Data Protection Act, individuals have the following rights:
· right of subject access (further information see below);
· right to prevent processing likely to cause harm or distress;
· right to prevent processing for the purposes of direct marketing;
· rights in relation to automated decision taking;
· right to take action for compensation if the individual suffers damage;
· right to take action to rectify, block, erase or destroy inaccurate data; and
· right to make a request to the Information Commissioner for an assessment to be made as to whether any provision of the Act has been contravened.

Subject Access

Individuals whose information is held by the Practice have rights of access (with exemptions) to it, regardless of the way in which the information may be held/retained. Refer to Records Management Policy.

The Practice will ensure an up to date procedure is in place to deal with requests for access to information. The Access to Health Records Act 1990 provides access rights to those who may have a claim, to deceased patients records as the Data Protection Act only relates to living individuals.

Complaints

Individuals have a right to complain if they believe that the Practice is not complying with the requirements of the Data Protection legislation. The Practice will implement the use of the Practice Complaints Procedure to deal with complaints arising from a breach or suspected breach of the Data Protection Act 1998. If the complainant is dissatisfied with the conduct of the Practice or the outcome of the complaints procedure, they can be referred to the Information Commissioner.

Principle 7

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of person identifiable data and against accidental loss or destruction of, or damage to, person identifiable data

All Person identifiable data held or processed by the Practice as a Data Processor, will be held and processed in accordance with this principle, which states that person identifiable data must be processed and handled safely and securely.

Principle 8

Person identifiable data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of person identifiable data

If staff are required to send personal identifiable information in a computer readable format to a country outside of the EEA, this must not be done without the specific agreement of the Practice Head of Information Governance/Caldicott Guardian, as the levels of protection for such information may not be as comprehensive as those in the UK. Similar safeguards must be taken for manual records.

7 Policy Principles

The principles of this Data Protection Policy are:
The Practice will implement appropriate organisational and technical measures to ensure that:

Person identifiable data processed by the Practice is treated in accordance with the requirements of the Data Protection Act 2018, in order to ensure that:

- Data Subjects' rights in terms of Article 8 of the Human Rights Act of 2018, the right to "respect for private and family life", are upheld across all flows of Person identifiable data in the Practice's control;
- Planning of organisational and service activity will be undertaken in conjunction with a formal Privacy Impact Assessment to determine appropriate, effective and affordable Data Protection controls, and to implement them across the Practice;
- The quality and integrity of recorded Person identifiable data will be developed and maintained to ensure that it is fit for the purposes for which it was collected; and
- Compliance with the regulatory framework will be audited, monitored and maintained.

8 Definitions

The following terms are used in the Data Protection Act 2018 and this policy, with specific meanings as described:

8.1 Data
Section 1(1) of the 2018 Data Protection Act defines 'data' as: Information which -
a) Is being processed by means of equipment operating automatically in response to instructions given for that purpose;
b) Is recorded with the intention that it should be processed by means of such equipment;
c) Is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system;
d) Does not fall within paragraph (a), (b) or (c) but forms part of an accessible record; or
e) Is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d).

8.2 Relevant Filing System
A relevant ‘filing system’ is defined in (s.1(1)) as:
‘Any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.’

8.3 Accessible Records
Paragraph (d) of the definition of ‘data’ includes accessible records. Section 68 of the Act defines accessible records as a health record, and educational record or an accessible public record. In the context of this policy, the terms “information” and “data” refer to any item of person identifiable data about living individuals, held in “accessible records” including manual files, computer databases, videos and other automated media, such as personnel and payroll records, medical records, other manual files, microfiche/film, pathology results, prescriptions, photographs, x-rays, scans and even telephone recordings and emails.

8.4 Data Subject
A ’data subject’ is defined as any individual who can be identified using the information or data held, i.e. the “subject” of the data, or from combinations of the data and other information which the data Controller has, or is likely to have in future.

8.5 Person identifiable data
Person identifiable data’ is defined in schedule 1(1) as:
Data which relate to a living individual who can be identified:
a) from those data, or
b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual’.

8.6 Sensitive Person identifiable data
Sensitive Person identifiable data’ is defined in schedule 2 as person identifiable data relating to any one or more of the following:
· Racial or ethnic origin
· Political opinions
· Religious or other beliefs of a similar nature
· Trades Union membership
· Physical or mental health conditions
· Sexual life
· The commission or alleged commission by the data subject of any offence
· Any proceedings for any offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.

Data Controllers are forbidden from processing sensitive person identifiable data unless one or more of 17 specified conditions are met. These conditions are:
1. Explicit consent;
2. Employment law obligations;
3. Vital interests of the data subject or another person where consent cannot be given or unreasonably withheld;
4. Not-for-profit organisation existing for political, philosophical, religious or trade union purposes, only relating to members and not disclosed to third parties without consent;
5. Information deliberately made public by the data subject;
6. Legal rights;
7. Public functions (administration of justice, etc.);
8. Medical purposes by a health professional;
9. Racial or ethnic records for the purpose of racial equality;
10. Prevention or detection of crime;
11. Apprehension or prosecution of offenders;
12. Required, authorised by or under enactment, by rule of law or by the order of a court;
13. Protection of the public;
14. Substantial public interest disclosure;

15. Insurance and pensions – family data
16. Insurance and pensions – processing
17. Medical research

8.7 Data Controller
A ‘data controller’ is a ‘person who (either alone or jointly or in common with other persons) determines the purpose for which and the manner in which any person identifiable data are, or are to be, processed’ (s. 1(1)).

8.8 Processing
‘Processing’, in relation to information or data, means:
Obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including —
· organisation, adaptation or alteration of the information or data,
· retrieval, consultation or use of the information or data,
· disclosure of the information or data by transmission, dissemination or otherwise making available, or
· alignment, combination, blocking, erasure or destruction of the information or data.
This definition of ‘processing’ is so broad as to include, for all practical purposes, anything that is done with information, including simply calling it up on a computer screen, reading a manual file, moving information over a network, email or on a portable memory device, and even includes recording of photographic or CCTV images and telephone recordings.

8.9 Notification
The Practice is required by the Act to ‘notify’ the Information Commissioner of all processing that takes place within the organisation, including each class of information processed, and the purpose for which it is processed. Any changes to the classes of information processed, or the reasons for processing must be registered with the Information Commissioner by the Trust Data Controller.

9 Service User and Staff Information

All staff and service user information, whether it is held manually or in an automated system, will be kept secure in accordance with the Practice’s Records Management and Information Security Policies.

9.1 Service Users
All service users must be provided with information on the use and disclosure of confidential information about them that is held by the Practice.

- Staff should make sure that information leaflets on patient confidentiality and information disclosure are available in a format that is understandable to the service user, and staff should check, where practicable, that service users have read and understood the leaflets.
- Staff should make clear to service users, in a way that is appropriate to that individual, when information is recorded and under what circumstances the health record will be accessed.
- Staff must check that patients are aware of the choices available to them and that they have the right to choose whether or not to agree to information that they have provided in confidence being shared.
- Staff should communicate effectively with service users to ensure they understand what the implications may be if they choose to restrict the disclosure of certain information.
- Patient information leaflets and posters have been produced and are available upon request and sited in patient areas.

9.2 Staff
All members of staff are Data Subject’s under the Act.
Any member of staff, current, past or potential (applicant) who wishes to have a copy of the information the Practice holds on them under the subject access provisions of the Data Protection Act must make an application in writing to the Data Protection Officer of the Practice.
There are subject access procedures outlining the process to follow to deal with such requests.

9.3 Sharing and Disclosure of Service User Information
All Data Controllers wishing to participate in information sharing agreements with Practice will be required to sign up to the most recent version of the Information Sharing Principles Protocol.

This agreement has been produced in conjunction with organisations in the NHS, Social Services and partner organisations. This agreement is to be supported by “second tier” Information Sharing Agreement s (produced by CIOSPCT) for each flow of person identifiable data.
These second tier agreements will describe the data sets to be shared, the mechanism for sharing, and the roles of the originating and receiving Data Controller.

9.4 Subject Access Requests
Section seven (7) of the Act allows an individual to:
· Be informed by any data controller whether person identifiable data of which that individual is the data subject are being processed by or on behalf of that data controller.
· And if is the case to, to be given by the data controller a description of:
· The person identifiable data of which that individual is the data subject;
· The purposes for which they are being or are to be processed and;
· The recipients or classes of recipients to whom they are or may be disclosed.
To have communicated to him in an intelligible form:
· The information constituting any person identifiable data of which that individual is the data subject; and
· any information available to the data controller as to the sources of those data.
The Service User can obtain this information from the Practice by making a written request. This is known as a ‘Subject Access Request’. The Practice’s approach to dealing with Subject Access
Requests by service users or staff is detailed in the Subject Access Request Policy and Procedure.

10 Staff Training
The Practice will provide appropriate training and awareness programs to ensure staff are aware of their responsibilities for Data Protection, Confidentiality and Information Security. These awareness initiatives will be included in the Practice’s Core Induction programme, and will be presented by the Caldicott Guardian or the Information Governance Manager.
All new starters at the Practice will be required to attend mandatory Information Governance training as part of the Practice induction process.
A register will be maintained of all staff attendance at induction and other training sessions.

11 Contracts of Employment
The Practice Manager is to ensure that all staff have valid contracts of employment which will include specific clauses for Data Protection and Confidentiality.

12 Disciplinary Procedures and Enforcement
Breaches of this Data Protection Policy will be addressed through the Practice’s Disciplinary Procedures.

13 Standards
This policy and related procedures or protocols will be assessed in terms of the standards defined in the Data Protection Act of 1998, and the Department of Health publication - Confidentiality: NHS Code of Practice.

14 Monitoring
This policy will be monitored and audited by the Information Governance Manager in accordance with the requirements stated in the Overarching Information Governance Policy.