UK General Data Protection Regulation Policy

DOCUMENT CONTROL:

Confidentiality Notice:

This document and the information contained therein is the property of Wootton Medical Centre.

This document contains information that is privileged, confidential or otherwise protected from disclosure. It must not be used by, or its contents reproduced or otherwise copied or disclosed without the prior consent in writing from Wootton Medical Centre.

Document Details:

Policy:	UK General Data Protection Regulation Policy
Author & Role:	
Organisation:	Wootton Medical Centre
Document Reference:	
Current Version Number:	
Current Document Approved By:	Lisa Marotta
Date Approved:	06.11.23

Document Revision & Approval History

Version	Date	Version Created By:	Version Approved By:	Comments
1	06.11.23	Jude Michie	Lisa Marotta	New policy
2				
3				

Table of contents

1 Introduction 4

1.1 Policy statement 4

1.2 Status 4

1.3 Training and support 4

2 Scope 4

2.1 Who it applies to 4

2.2 Why and how it applies to them 5

3 Definition of terms 5

3.1 Consent 5

3.2 Data Protection Act 2018 5

3.3 Data protection by design and default 5

3.4 Data Protection Officer 5

3.5 Data controller 5

3.6 Data processor 6

3.7 Data subject 6

3.8 UK General Data Protection Regulation (UK GDPR) 6

3.9 Personal data 6

3.10 Personal data breach 6

3.11 Processing 6

3.12 Pseudonymisation 6

3.13 Recipient 6

3.14 Third party 7

4 Introduction of the UK GDPR 7

4.1 Background 7

4.2 UK GDPR and DPA18 7

5 Data protection by design and default 7

5.1 Data protection by design 7

5.2 Data protection by default 7

6 Roles of data controllers and processors 8
6.1 Data controller 8
6.2 Data processor 9

7 Data subjects' rights 9
7.1 Overview 9
7.2 Right to be informed 9
7.3 Right of access 10
7.4 Right to rectification 10
7.5 Right to erasure 10
7.6 Right to restrict processing 11
7.7 Right to data portability 11
7.8 Right to object 11
7.9 Rights in relation to automated decision making and profiling 11

8 Subject access requests 11
8.1 Recognising subject access requests 11
8.2 Responding to a subject access request 12
8.3 Fees 12
8.4 Verifying the subject access request 12
8.5 Supplying the requested information 12
8.6 Third party requests 13
8.7 Requests from solicitors 13
8.8 Requests from insurers 13
8.9 Refusing to comply with a SAR 13

9 Data breaches 14
9.1 Data breach definition 14
9.2 Reporting a data breach 14
9.3 Notifying a data subject of a breach 15

10 Consent 15
10.1 Appropriateness 15
10.2 Obtaining consent 15
10.3 Parental consent 16

11 Data mapping and Data Protection Impact Assessments 16
11.1 Data mapping 16
11.2 Data mapping and the Data Protection Impact Assessment 16
11.3 Data Protection Impact Assessment 16
11.4 Data Protection Impact Assessment process 17

12 Information asset register 18

13 Summary **18**

Annex A – The Data Protection Impact Assessment (DPIA) **20**

Annex B – The Data protection impact assessment process **22**

Annex C – UK GDPR checklist **44**

1 Introduction

1.1 Policy statement

The UK General Data Protection Regulation (UK GDPR herein) came into force on 1 January 2021 and is incorporated in the Data Protection Act 2018 (DPA18) at part 2.

The UK GDPR applies to all organisations in the UK (with the exception of law enforcement and intelligence agencies) and Wootton Medical Centre (WMC) must be able to demonstrate compliance at all times. Understanding the requirements of the UK GDPR will ensure that the personal data of both staff and patients is protected accordingly.

1.2 Status

The WMC aims to design and implement policies and procedures that meet the diverse needs of our service and workforce, ensuring that none are placed at a disadvantage over others, in accordance with the Equality Act 2010. Consideration has been given to the impact this policy might have regarding individual protected characteristics of those to whom it applies.

This document and any procedures contained within it are non-contractual and may be modified or withdrawn at any time. For the avoidance of doubt, it does not form part of your contract of employment.

1.3 Training and support

WMC will provide guidance and support to help those to whom it applies to understand their rights and responsibilities under this policy. Additional support will be provided to managers and supervisors to enable them to deal more effectively with matters arising from this policy.

2 Scope

2.1 Who it applies to

This document applies to all employees, partners and directors of the practice. Other individuals performing functions in relation to the surgery, such as agency workers, locums and contractors, are encouraged to use it.

Furthermore, it also applies to clinicians who may or may not be employed by the organisation but who are working under the Additional Roles Reimbursement Scheme (ARRS).[1]

2.2 Why and how it applies to them

All personnel at Wootton Medical Centre have a responsibility to protect the information they process. This document has been produced to enable all staff to understand their individual and collective responsibilities in relation to the UK GDPR.

3 Definition of terms

3.1 Consent

Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.[2]

3.2 Data Protection Act 2018

The Data Protection Act 2018 (DPA 2018) sets out the framework for data protection law in the UK. It sits alongside and supplements the UK General Data Protection Regulation (UK GDPR).[3]

3.3 Data protection by design and default

Data protection by design and default means putting in place appropriate technical and organizational measures to implement the data protection principles effectively and safeguard individual rights.[4]

3.4 Data Protection Officer

An expert on data privacy, working independently to ensure compliance with policies and procedure

3.5 Data controller

[1] Network DES specification 2022/23
[2] Article 4 UK GDPR
[3] ICO About the DPA 2018
[4] ICO Guide to the UK General Data Protection Regulation

The natural or legal person, public authority, agency or other body that, alone or jointly with others, determines the purposes and means of the processing of personal data[5]

3.6 Data processor

A natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller[2].

3.7 Data subject

The identified or identifiable living individual to who personal data relates[6]

3.8 UK General Data Protection Regulation (UK GDPR)

The UK GDPR sets out the key principles, rights and obligations for most processing of personal data in the UK.[4]

3.9 Personal data

Information that relates to an identified or identifiable individual[7]

3.10 Personal data breach

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.[2]

3.11 Processing

Any operation or set of operations that is performed on personal data or on sets of personal data whether or not by automated means such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

3.12 Pseudonymisation

Pseudonymisation is a technique that replaces or removes information in a data set that identifies an individual.[7]

3.13 Recipient

The entity to which personal data is disclosed

[5] ICO Definitions

[7] ICO What is personal data

3.14 Third party

A third party means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data[2].

4 Introduction of the UK GDPR

4.1 Background

The UK GDPR was introduced on 1 January 2021 and is largely based on the EU GDPR which had applied in the UK since 25 May 2018.

4.2 UK GDPR and DPA18

The UK GDPR is incorporated in the DPA18 at Part 2.

5 Data protection by design and default

5.1 Data protection by design

Data protection by design is ultimately an approach that ensures that privacy and data protection issues are considered at the design phase of any system, service, product or process and then throughout the lifecycle.[4]

Wootton Medical Centre will demonstrate data protection by design by:

- Conducting a data protection impact assessment (DPIA)
- Ensuring there are privacy notices on the website and in the waiting rooms which are written in simple, easy-to-understand language
- Adhering to Articles 25(1) and 25(2) of the UK GDPR[8]
- Adhering to Section 6.1 of this policy

Data protection by design is a legal requirement.

5.2 Data protection by default

Data protection by default is an approach that ensures that data is processed only for the achievement of a specific purpose.[4]

Wootton Medical Centre will demonstrate data protection by default by:

[8] Article 25 UK GDPR

- Processing data only for the purpose(s) intended
- Ensuring consent is obtained from the data subject prior to data being processed
- Providing patients access to their data on request (Subject Access Requests)
- Ensuring patients consent to access of their data by third parties
- Processing data in a manner that prevents data subjects being identified unless additional information is provided (using a reference number as opposed to names – pseudonymisation)
- Processing data in accordance with section 6.2 of this policy

Through effective data protection Wootton Medical Centre will remain compliant with the UK GDPR.

6 Roles of data controllers and processors

6.1 Data controller

At Wootton Medical Centre, the role of the data controller is to ensure that data is processed in accordance with Article 5 of the UK GDPR. He/she should be able to demonstrate compliance and is responsible for making sure that data is:[9]

- Processed lawfully, fairly and in a transparent manner in relation to the data subject
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which the data is processed
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data, which is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay
- Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

[9] Article 5 Principles relating to processing of personal data

6.2 Data processor

Data processors are responsible for the processing of personal data on behalf of the data controller. Processors must ensure that processing is lawful and that at least one of the following applies:[10]

- The data subject has given consent to the processing of his/her personal data for one or more specific purposes
- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract
- Processing is necessary for compliance with a legal obligation to which the data controller is subject
- Processing is necessary in order to protect the vital interests of the data subject or another natural person
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller
- Processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child

At Wootton Medical Centre, all staff are classed as data processors as their individual roles will require them to access and process personal data.

7 Data subjects' rights

7.1 Overview

All data subjects have the following rights[11]:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling

7.2 Right to be informed

[10] Article 6 Lawfulness of processing
[11] ICO - Individual Rights

In accordance with Articles 13 and 14 of the UK GDPR, Wootton Medical Centre is obliged to advise data subjects of the purposes for processing their data, the retention periods for the data and who this data will be shared with. This is referred to as privacy information.

7.3 Right of access

Wootton Medical Centre ensures that all patients are aware of their right to access their data and has privacy notices displayed in the following locations:

- Waiting room
- Website
- Information leaflet

To comply with the UK GDPR, all organisation privacy notices are written in a language that is understandable to all patients and meet the criteria detailed in Articles 12, 13 and 14 of the UK GDPR.

The reason for granting access to data subjects is to enable them to verify the lawfulness of the processing of data held about them. In addition, data subjects can authorise third party access, e.g., for solicitors and insurers, under the UK GDPR.

7.4 Right to rectification

In accordance with Article 16 of the UK GDPR, data subjects have the right to have inaccurate personal data rectified and/or incomplete personal data completed. At Wootton Medical Centre, should a clinician enter a diagnosis that is later proved incorrect, the medical record should retain both the initial diagnosis and the subsequent accurate diagnosis with text to make it clear that the diagnosis has been updated.

Patients can exercise their right to challenge the accuracy of their data and request that this is corrected. Should a request be received, the request should state the following:

- What is believed to be inaccurate or incomplete
- How this practice should correct it
- If able to, provide evidence of the inaccuracies

A request can be verbal or in writing and the Information Commissioner's Office (ICO) recommends that any request is followed up in writing as this will allow the requestor to explain their concerns, give evidence and state the desired solution. Additionally, this will also provide clear proof of the requestor's actions, should they decide to challenge this organisation's initial response.

Detailed guidance from the ICO can be accessed here.

7.5 Right to erasure

In accordance with Article 17 of the UK GDPR, data subjects have the right to have personal data erased (this is also referred to as the right to be forgotten). This right

permits a data subject to request personal data is deleted in situations where there is no compelling reason to retain the data.

The BMA states: “Whilst it will be extremely rare for information to be deleted from medical records, it is established practice that corrections or amendments can be made; however, the original information, along with an explanation as to why information has been corrected or amended, must remain as an audit trail.”

This organisation will adhere to the BMA Access to Health Records Guidance.

Where Wootton Medical Centre has shared information with a third party, there is an obligation to inform the third party about the data subject’s request to erase their data providing it is achievable and reasonably practical to do so. Detailed guidance can be accessed here.

7.6 Right to restrict processing

In accordance with Article 18 of the UK GDPR, individuals have the right to restrict the processing of their personal data. This applies in certain circumstances, with the aim being to enable the individual to limit the way an organisation processes (uses) their data. This right can be used as an alternative to the right to erasure.

7.7 Right to data portability

The right to data portability permits data subjects to receive and reuse their personal data for their own purposes and across different services.

7.8 Right to object

In accordance with Article 21 of the UK GDPR, individuals have the right to object to the processing of their personal data at any time.

At Wootton Medical Centre, individuals are requested to provide specific reasons why they object to the processing of their data. If the reasons are not an absolute right, this organisation can refuse to comply.

Refer to the ICO guidance for detailed information.

7.9 Rights in relation to automated decision making and profiling

In accordance with Article 22 of the UK GDPR, Wootton Medical Centre, is not permitted to make solely automated decision making. This includes profiling.

8 Subject access requests

8.1 Recognising subject access requests

At this organisation, data subjects are encouraged to use the subject access request (SAR) form which is included in the Access to medical records policy. All staff must note that the ICO state:

"An individual can make a SAR verbally or in writing, including on social media. A request is valid if it is clear that the individual is asking for their own personal data."

Any requests not using the SAR form, must be processed.

8.2 Responding to a subject access request

In accordance with the UK GDPR, data controllers must respond to all data subject access requests within one month of receiving the request. It is the guidance of the ICO that a universal approach is applied and a 28-day response time implemented.[12]

At Wootton Medical Centre, the 28-day response time applies.

In the case of complex or multiple requests, the data controller may extend the response time by a period of two months. In such instances, the data subject must be informed and the reasons for the delay explained.

Should the request involve a large amount of information, the data controller will ask the data subject to specify what data they require before responding to the request. Data controllers are permitted to 'stop the clock' in relation to the response time until clarification is received.

8.3 Fees

Under the UK GDPR, Wootton Medical Centre is not permitted to charge data subjects for initial access; this must be done free of charge. In instances where requests for copies of the same information are received or requests are deemed "unfounded, excessive or repetitive", a reasonable fee may be charged. However, this does not permit the organisation to charge for all subsequent access requests.[13]

The fee is to be based on the administrative costs associated with providing the requested information.

8.4 Verifying the subject access request

It is the responsibility of the data controller to verify all requests from data subjects using reasonable measures.

The use of the practice's Subject Access Request (SAR) form supports the data controller in verifying the request. In addition, the data controller is permitted to ask for evidence to identify the data subject, usually by using photographic identification, i.e., driving licence or passport.

8.5 Supplying the requested information

The decision on what format to provide the requested information in should take into consideration the circumstances of the request and whether the individual can access the data in the format provided.

[12] ICO Right of access

[13] BMA Guidance – Access to health records

Should an individual submit a SAR electronically, Wootton Medical Centre will reply in the same format (unless the data subject states otherwise).

8.6 Third party requests

At WMC, the data controller must be able to satisfy themselves that the person requesting the data has the authority of the data subject.

The responsibility for providing the required authority rests with the third party and is usually in the form of a written statement or consent form, signed by the data subject. A standard consent form has been issued by the BMA and Law Society of England and Wales and Wootton Medical Centre will request that third parties complete this form.

8.7 Requests from solicitors

At Wootton Medical Centre, requests are received from third parties such as solicitors. It is the responsibility of the third party to provide evidence that they are permitted to make a SAR on behalf of their client. If concern or doubt arises,
this organisation will contact the patient to explain the extent of disclosure sought by the third party.

Wootton Medical Centre can then provide the patient with the data as opposed to directly disclosing it to the third party. The patient is then given the opportunity to review their data and decide whether they are content to share the information with the third party.

8.8 Requests from insurers

SARs are not appropriate should an insurance company require health data to assess a claim. The correct process for this at Wootton Medical Centre is for the insurer to use the Access to Medical Reports Act 1988 (AMRA) when requesting a GP report.
The following fees are applicable:[14]

- GP report for insurance applicants £104.00
- GP supplementary report £27.00

8.9 Refusing to comply with a SAR

WMC will only refuse to comply with a SAR where exemption applies or when the request is manifestly unfounded or manifestly excessive. In such situations, the data controller will inform the individual of:

- The reasons why the SAR was refused
- Their right to submit a complaint to the ICO
- Their ability to seek enforcement of this right through the courts

[14] BMA Guidance – Fees for insurance reports and certificates

Each request must be given careful consideration and should Wootton Medical Centre refuse to comply, this must be recorded and the reasons for refusal justifiable.

9 Data breaches

9.1 Data breach definition

A data breach is defined as a security incident that has affected the confidentiality, integrity or availability of personal data.[15]

Examples of data breaches include:

- Access by an unauthorised third party
- Deliberate or accidental action (or inaction) by a data controller or processor
- Sending personal data to an incorrect recipient
- Loss or theft of computer devices containing personal data
- Alteration of personal data without permission
- Loss of availability of personal data

Examples of data breaches can be found on the ICO website.

9.2 Reporting a data breach

At Wootton Medical Centre, should any member of staff become aware of a data breach, they are, where possible, to contain the breach and advise their line manager immediately.

When determining whether this organisation needs to report the data breach to the ICO, this decision is to be based on whether or not the breach is a high risk to an individual's rights and freedoms. If this is deemed to be the case, then the ICO will need to be notified.

Whatever decision is made, this organisation must be able to justify the decision.

Breaches are to be reported to the ICO without undue delay or within 72 hours of becoming aware of the breach. Wootton Medical Centre will report the breach using the Data Security and Protection Incident Reporting Tool.

Failure to report a breach can result in a fine of up to £8.7m. It is therefore imperative that there are effective processes in place at WMC to detect, investigate and report breaches accordingly.

The data controller is to ensure that all breaches at Wootton Medical Centre are recorded. Article 33 of the UK GDPR outlines the requirements which include:

- Recording the facts pertaining to the breach
- The effects the breach has had on individuals or organisations
- Any remedial action(s) that have been completed
- The cause of the breach i.e., system or human error

[15] ICO – Personal data breaches

- Considering what system or process changes may be required to prevent future incidences

9.3 Notifying a data subject of a breach

The data controller must notify a data subject of a breach that has affected their personal data without undue delay. If the breach is high risk (i.e., a breach that is likely to have an adverse effect on an individual's rights or freedoms), then the data controller is to notify the individual before they notify the ICO.

The primary reason for notifying a data subject of a breach is to afford them the opportunity to take the necessary steps in order to protect themselves from the effects of a breach.

When the decision has been made to notify a data subject of a breach, the data controller at this organisation is to provide the data subject with the following information in a clear, comprehensible manner:

- The circumstances surrounding the breach
- The details of the person who will be managing the breach
- Any actions taken to contain and manage the breach
- Any other pertinent information to support the data subject

10 Consent

10.1 Appropriateness

The UK GDPR states that consent must be unambiguous and requires a positive action to "opt in" and it must be freely given. Data subjects have the right to withdraw consent at any time.

10.2 Obtaining consent

Consent is one of the lawful bases of processing and is appropriate if data processors are in a position to "offer people real choice and control over how their data is used".[16] If it is deemed appropriate to obtain consent, the following must be explained to the data subject:

- Why the organisation wants the data
- How the data will be used by the organisation
- The names of any third party data controllers with whom the data will be shared
- Their right to withdraw consent at any time

All requests for consent are to be recorded, with the record showing:

- The details of the data subject consenting
- When they consented

[16] ICO Consent

- How they consented
- What information the data subject was told

Consent is to be clearly identifiable and separate from other comments entered into the healthcare record. At this organisation, it is the responsibility of the data controller to demonstrate that consent has been obtained. Furthermore, the data controller must ensure that data subjects (patients) are fully aware of their right to withdraw consent and must facilitate withdrawal as and when it is requested.

10.3 Parental consent

The DPA 2018 states that parental consent (in relation to personal data) is required for a child under the age of 13. Additionally, the principle of Gillick competence remains unaffected and parental consent is not necessary when a child is receiving counselling or preventative care.

11 Data mapping and Data Protection Impact Assessments

11.1 Data mapping

Data mapping is a means of determining the information flow throughout an organisation. Understanding the why, who, what, when and where of the information pathway will enable Wootton Medical Centre to undertake a thorough assessment of the risks associated with current data processes.

Effective data mapping will identify what data is being processed, the format of the data, how it is being transferred, if the data is being shared and where it is stored (including off-site storage if applicable).

11.2 Data mapping and the Data Protection Impact Assessment

Data mapping is linked to the Data Protection Impact Assessment (DPIA) and, when the risk analysis element of the DPIA process is undertaken, the information ascertained during the mapping process can be used.

Data mapping is not a one-person task. All staff at Wootton Medical Centre will be involved in the mapping process thus enabling the wider gathering of accurate information.

11.3 Data Protection Impact Assessment

The DPIA is the most efficient way for this practice to meet its data protection obligations and the expectations of its data subjects. DPIAs are also commonly referred to as Privacy Impact Assessments or PIAs.

In accordance with Article 35 of the UK GDPR, a DPIA should be undertaken where:

- A type of processing, in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller

shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks

- Extensive processing activities are undertaken, including large scale processing of personal and/or special data

DPIAs are to include the following:

- A description of the processing operations, including the purpose of processing
- An evaluation of the need for the processing in relation to the purpose
- An assessment of the associated risks to the data subjects
- Existing measures to mitigate and control the risk(s)
- Evidence of compliance in relation to risk control

It is considered best practice to undertake DPIAs for existing processing procedures to ensure that Wootton Medical Centre meets its data protection obligations. DPIAs are classed as "live documents" and processes should be reviewed continually. As a minimum, a DPIA should be reviewed every three years or whenever there is a change in a process that involves personal data.

11.4 Data Protection Impact Assessment process

The DPIA process is illustrated in diagrammatic form below:

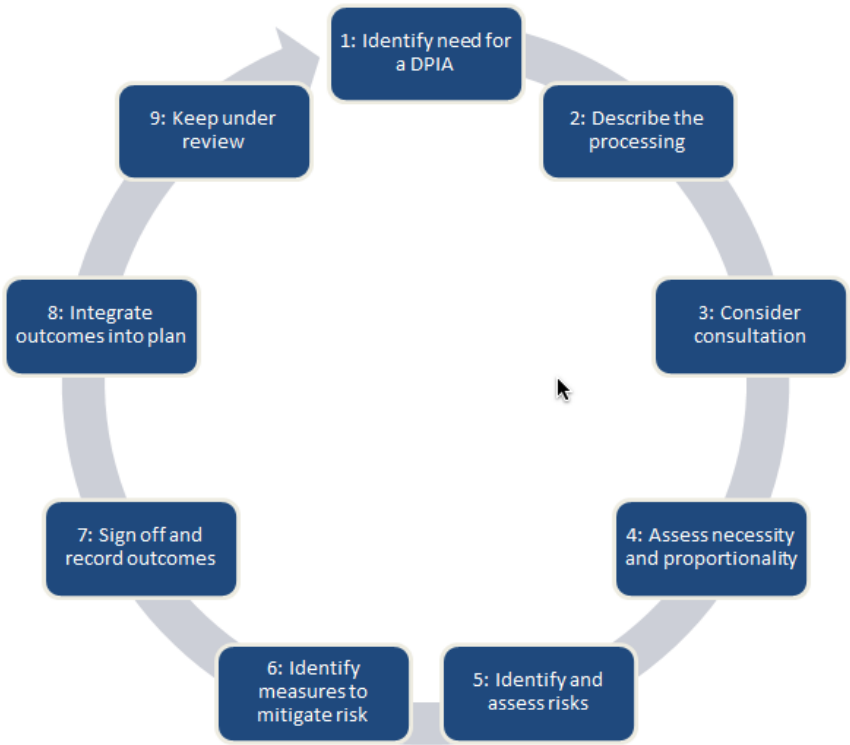

Image source: ico.org.uk

12 Information asset register

An information asset register (IAR) is a repository for similar or specific types or information and these repositories can be either physical or virtual. They include records management, cloud storage or backup systems, email services or even manual filing cabinets. Any repository where data is stored or processed is deemed to be an information asset.

In terms of information governance, the IAR reflects the risks and potential outcomes that are possible should that asset become lost or compromised. An IAR is a simple way to help understand and manage the organisation's information assets – i.e., what the organisation has, where they are, how they are secured and who has access to them.

Data has both value and risk so, from a commercial point of view and a governance point of view, having an IAR really is essential. It should state who is specifically responsible for each information asset, i.e., the information asset owner. For larger organisations, the various assets could have different owners which should be recorded on the register.

The register must note whether the asset contains personally identifiable information and whether that information includes any 'sensitive' or 'special category' personal data.

WMC will ensure appropriate procedures are in place for effective information risk management and provide the structural means to identify, prioritise and manage the risks involved in all information activities. Measures will be taken to ensure that each system is secured to an appropriate level and that data protection principles are maintained.

Maintaining an accurate asset register supports the process of effectively managing assets within the organisation, minimises risk and always encourages staff to work securely.

13 Summary

Given the complexity of the UK GDPR, all staff at Wootton Medical Centre must ensure that they fully understand the requirements within the regulation.

Understanding the regulation will ensure that personal data at this practice remains protected and the processes associated with this data are effective and correct.

Annex A – The Data Protection Impact Assessment (DPIA)

WHEN TO CARRY OUT A DPIA

The DPIA identifies and assesses privacy implications where information (data) about individuals is collected, stored, transferred, shared, and managed. It should be process rather than output orientated.

The purpose is to have the potential to detect and mitigate information risks, as well as to modify plans accordingly.

A DPIA should be completed when the following activities occur:

- Developing or procuring any new programme, policy, procedure, service, technology or system ("project") that handles or collects information relating to individuals

- Developing revisions to an existing programme, policy, procedure, service, technology or system which significantly change how information is managed

The General Data Protection Regulation (GDPR) became law on 24th May 2016, it is a single EU-wide regulation on the protection of confidential and sensitive information. It entered into force on the 25th May 2018, repealing the Data Protection Act (1998).

The Regulation in Article 35 (recitals 84, 89, 90, 91, 92, 93, 95) makes it obligatory to perform a Data Protection impact assessment in case of large-scale processing of special categories of data (as in this case health data and genetic data see article 9(1). This could help to ascertain the legal basis for processing, which will be helpful for public authorities now that the open door of ‘legitimate interests’ is closed. It is also important to note that “a single assessment may address a set of similar processing operations that present similar high risks”. This could significantly help in reducing the administrative burden for hospitals and health and care providers when performing such an assessment.

A data protection impact assessment shall in particular be required in the case of:

(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

(b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or

(c) a systematic monitoring of a publicly accessible area on a large scale.

This DPIA has been designed to meet the requirements of current legislation and common law duties and the expanded requirements of the GDPR as above, however Consent modelling/Fair Processing modification should be addressed by separate GDPR action plans and strategies as several of the policies currently in use will need to be updated to reflect legislative changes.

Annex B – The Data protection impact assessment process

STEP 1 – PROJECT DETAILS

Project Name/Title	
Description and Purpose of the Initiative – *Include how many individuals will be affected by the initiative*	
Details of any link to any wider initiative *(if applicable)*	
Stakeholder Analysis *List those who may be affected (stakeholders have been consulted prior to project start), e.g., service users, clients, staff-managers and practitioners, trade unions, visitors, professional organisations, IT providers, regulators and inspectorial bodies, MPs, councillors, partner organisations, media, carers*	**Internal:** **External:**

Does the initiative involve the use of existing personal and/or confidential data: • **For new purposes?** • **In different ways?** **If so, please explain** *(if not already covered above)*	
Are potential new purposes likely to be identified as the scope of the initiative expands?	
What is already available? *(Any previous PIA, research or consultation undertaken)*	

STEP 2 – CONTACTS

Who is completing this assessment?	
Name	
Job Title	
Department/Directorate name	
Contact Address	
Email Address	
Telephone Number	
Connection to Project	

Other person(s) with responsibility for this initiative e.g., project manager/director, senior information risk owner (SIRO)	
Name	
Job title	
Department/directorate name	
Contact address	

Email address	
Telephone number	
Connection to project	

Technical lead(s) *(if relevant)*	
Name	
Email address	
Telephone number	

STEP 3 – SCREENING QUESTIONS

The purpose of these questions is to establish whether a full privacy impact assessment is necessary and to help to draw out privacy considerations					
		Yes	**No**	**Unsure**	**Comments** *(Document initial comments on privacy impacts or clarification for why this is not an issue or why you are unsure)*
i	Is the information about individuals likely to raise privacy concerns or expectations e.g., health records, criminal records or other information people would consider particularly private?				

ii	Will the initiative involve the collection of new information about individuals?				
iii	Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?				
iv	Will the initiative require you to contact individuals in ways which they may find intrusive[17]?				
v	Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?				
vi	Does the initiative involve you using new technology which might be perceived as being privacy intrusive e.g., biometrics or facial recognition?				
vii	Will the initiative result in you making decisions or taking action against individuals in ways which can have a significant impact on them?				

[17] Intrusion can come in the form of collection of excessive personal information, disclosure of personal information without consent and misuse of such information. It can include the collection of information through the surveillance or monitoring of how people act in public or private spaces and through the monitoring of communications whether by post, phone or online and extends to monitoring the records of senders and recipients as well as the content of messages

viii	Will the initiative compel individuals to provide information about themselves?				

If you answered **No** to all of the above screening questions and you can evidence/justify your answers in the comments box above, you do not need to continue with the DPIA.

Should the project at any point in the future use personal information you will need to revisit the screening questions and the DPIA.

If you answered or **Unsure** to any of the above, please continue with the DPIA.

STEP 4 – DATA COLLECTION

Please mark all information to be collected

Description	Specific data item (s)	Justification *(Reason that the data item(s) is/are needed)*
Personal details		
Family, lifestyle and social circumstances	*Marital/partnership status* *Next of kin* *Carers/relatives* *Children/dependents* *Social status e.g., housing*	

Description	Specific data item (s)	Justification *(Reason that the data item(s) is/are needed)*
Education and training details	*Education/qualifications* *Professional training* *Not applicable*	
Employment details	*Employment status* □ *Career details* □ *Other* □ *please specify:* *Not applicable* □	
Financial details	*Income* □ *Salary* □ *Bank details* □ *National Insurance number* □ *Benefits* □ *Other* □ *please specify:* *Not applicable* □	
Sensitive data: **Racial or ethnic origin**	*Racial/ethnic origin* □	

Description	Specific data item (s)	Justification *(Reason that the data item(s) is/are needed)*
Sensitive data: **Physical or mental health or condition** *NB.* *Includes treatment if applicable.* *Include Mental health status e.g., whether detained or voluntary under the Mental Health Act if applicable.*	List the data items: Not applicable □	
Sensitive data: **Sexual identity and life**	List the data items: Not applicable □	
Sensitive data: **Religious or other beliefs of a similar nature**	List the data items: Not applicable □	

Description	Specific data item (s)	Justification *(Reason that the data item(s) is/are needed)*
Sensitive data: **Trade union membership**	List the data items: Not applicable □	
Sensitive data: **Offences including alleged offences**	List the data items: Not applicable □	
Sensitive data: **Criminal proceedings, outcomes and sentences**	List the data items: Not applicable □	

STEP 5 – THE INFORMATION ASSET

How will the data be obtained and from where?	

How will the data be used?	
Will the data be used locally or nationally? *If national, list any available guidance*	
Who will be the owner of the information? **i.e., the Information Asset Owner (IAO)** *This is usually the director or service lead under which this asset sits*	
Who will be the Information Asset Administrator? (IAA) *This is usually the business manager or person with day-to-day access and control*	
Will a third party have access to the information? *If so, name the third party, the circumstances and details of how the data will be accessed*	

Will the data be shared with any other team or organisation? *If so, name the organisation and the circumstances* *If so, is there a data sharing agreement in place?*	

STEP 6 – DATA FLOWS

Please provide a process map or diagram if available, or complete the table below

The answer to most the questions for the data flows are the same, as described below.

Name of Flow	What is the purpose of the data flow?	Will you be receiving data or sending it or both?	Where will you be receiving it from and/or sending it to?	Is the data anonymised?	Is the data electronic or paper?	How is the data to be transferred? e.g., via a system, email, fax, post, by hand	How will the data be secured in transit? e.g., nhs.net to nhs.net	How often will data be transferred?	How many records in each transfer?	Where will the data be stored?	How will the data in storage be secured?

STEP 7 – DATA PROTECTION ACT COMPLIANCE

Name the data controller(s) *The data controller is the organisation which, alone or jointly or in common with other organisations, determines the purposes for which and the manner in which any personal data is, or is to be, processed.* *The data controller takes responsibility for complying with the GDPR.*	
Name any data processors and provide contact details *A data processor means any organisation which processes the data on behalf of the data controller.*	
What is the legal basis for processing the data? *e.g., consent, required by law, etc.*	

DATA PROTECTION ACT PRINCIPLES

Principle	Response	Actions required
Principle 1: Personal data shall be processed lawfully, fairly and in a transparent manner		
Individuals affected by the project must be informed about the processing of their data. Has a fair processing notice been provided or is a new or revised communication needed?		
What processes are in place to ensure that data required for secondary purposes is pseudonymised (or anonymised)?		
If you are relying on consent to process personal data, how will consent be obtained and recorded, what information will be provided to support the consent process and what will you do if permission is withheld or given but later withdrawn?		
Principle 2: Personal data shall be collected for specified, explicit and legitimate purposes		

Principle	Response	Actions required
What procedures are in place to ensure that privacy implications are considered prior to using data for a different purpose to that originally specified?		
Principle 3: Personal data shall be adequate, relevant and limited to what is necessary		
What procedures are in place for ensuring that data collection is adequate, relevant and not excessive in relation to the purpose for which data are being processed?		
How will you ensure that the data you are using is likely to be of good enough quality for the purposes it is used for?		
Principle 4: Personal data shall be accurate and where necessary kept up to date.		
What procedures are in place for ensuring that data collection is accurate?		
What procedures are in place for ensuring that data collection is kept up to date?		

Principle	Response	Actions required
What procedures are in place to correct inaccurate data when requested to do so by a data subject?		
Principle 5: Personal data shall be kept in a form which permits identification of the data subject for no longer than is necessary		
How long is the data to be retained for?		
What procedures are in place for: • Archiving • Anonymisation • Deletion • Destruction of the data?		
Are there likely to be any exceptional circumstances for retaining certain data for longer than the normal period(s)?		
What procedures are in place to provide data subjects access to their records?		

Principle	Response	Actions required
What procedures are in place to prevent the processing of data which may cause damage or distress?		
What procedures are in place for data subjects who may require the rectification, blocking, erasure or destruction of inaccurate data?		
Principle 6: Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss destruction or damage		
What procedures are in place to ensure that all staff who have access to the data undertake information governance training?		
What procedures are in place to ensure that data, whether at rest or in transit, is secured?		

Principle	Response	Actions required
What procedures are in place to prevent the unauthorised disclosure of data to third parties?		

COMMON LAW DUTY OF CONFIDENTIALITY

Assessment of compliance	
Has the individual to whom the information relates given consent?	
Is the disclosure in the overriding public interest?	
Is there a legal duty to do so, for example a court order?	
Is there a statutory basis that permits disclosure such as approval under Section 251 of the NHS Act 2006?	

HUMAN RIGHTS ACT 1998

The Human Rights Act establishes the right to respect for private and family life. Current understanding is that compliance with the Data Protection Act and the common law of confidentiality should satisfy Human Rights requirements.

Will your actions interfere with the right to privacy under Article 8? Have you identified the social need and aims of the project? Are your actions a proportionate response to the social need?

STEP 8 – PRIVACY ISSUES IDENTIFIED AND RISK ANALYSIS

Any privacy issues which have been identified during the DPIA process (for example: no legal basis for collecting and using the information; lack of security of the information in transit, etc.) should be documented in the risk register template embedded below. This risk register will enable you to analyse the risks in terms of impact and likelihood and document required action(s) and outcomes.

Note that where it is proposed that a privacy risk is to be 'accepted', approval for such acceptance should be sought from the Caldicott Guardian where patient data is concerned and the SIRO for all information risks.

STEP 9 – DATA PROTECTION PRINCIPLES COMPLIANCE AND AUTHORISATION

Please provide a summary of the conclusions that have been reached in relation to this project's overall compliance with the DPPs. This could include indicating whether some changes or refinements to the project might be warranted.

Information asset owner	**Name:**
	Date:

	Signature:
Reasoning behind the decision to accept or reject the identified privacy risks	
Data Protection Officer/Caldicott Guardian *(Caldicott Guardian only where the personal data is about patients)*	**Name:**
	Date:
	Signature:
Reasoning behind the decision to accept or reject the identified privacy risks	
Senior Information Risk Owner *(where the identified privacy risks are significant)*	**Name:**
	Date:
	Signature:
Reasoning behind the decision to accept or reject the identified privacy risks	
Information Governance Lead	**Name:**

	Date:
	Signature:
Reasoning behind the decision to accept or reject the identified privacy risks	

REFERENCES

- Data Protection Act 2018
- UK General Data Protection Regulations 2016
- The Caldicott Principles
- Common Law Duty of Confidentiality
- The Freedom of Information Act 2000
- The Mental Capacity Act 2005
- Section 251 of the NHS Act 2006 (originally enacted under Section 60 of the Health and Social Care Act 2001)
- Public Health (Control of Disease) Act 1984
- Public Health (Infectious Diseases) Regulations 1988
- The Gender Recognition Act 2004
- Confidentiality: NHS Code of Practice 2003
- IGA Records Management Code of Practice for Health and Social Care 2016
- Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013
- Abortion Regulations 1991
- Road Traffic Act 1988
- ICO Data Sharing Code of Practice
- Confidentiality and Disclosure of Information Directions 2013
- Health and Social Care Act 2012
- The Criminal Justice Act 2003
- The NHS Information Security Management Code of Practice 2007
- The Computer Misuse Act 1990
- The Electronic Communications Act 2000
- The Regulation of Investigatory Powers Act 2000
- The Prevention of Terrorism Act 2005
- The Copyright, Designs and Patents Act 1988
- The Re-Use of Public Sector Information Regulations 2005
- The Human Rights Act 1998
- The NHS Care Record Guarantee 2007

- Anonymisation Standard for Publishing Health and Social Care Data Code of Confidentiality

Annex C – UK GDPR checklist

This checklist has been designed to support managers in ensuring compliance with the UK GDPR.

Creating a culture of awareness	
All staff need to be aware that the UK GDPR became applicable by law in the UK as of the 1 January 2021 • It is essential that they have an understanding of the UK GDPR • Have you shared the organisation's UK GDPR policy with them or signposted them to further information, i.e., ico.org.uk?	
Action complete (✓ or ✗)	

Understanding the information flow	
The organisation must understand why, whose, what, when and where personal data is processed. • Conducting a data-mapping exercise will enable organisations to do this • Data-mapping is not a one-person task; all staff should be involved, enabling the wider gathering of accurate information	
Action complete (✓ or ✗)	

Data Protection Impact Assessment (DPIA)	
The DPIA is the most efficient way for the organisation to meet its data protection obligations. DPIAs are mandatory in accordance with Article 35 of the UK GDPR and should be undertaken when: • A type of processing, in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons; the data controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations which present similar high risks • Extensive processing activities are undertaken, including large scale processing of personal and/or special data Have DPIAs been completed? Best practice is to undertake DPIAs for existing processes to ensure that data protection obligations are met.	
Action complete (✓ or ✗)	
Updating privacy information	
All data subjects must understand how their data will be used. • Have you updated your practice privacy notice and are all staff aware of the changes?	

- Have you displayed the privacy notice in prominent positions such as the waiting room, consulting rooms and website and updated the organisation's information leaflet?
- Is your privacy notice in a language that is understandable to all patients?
- Does it comply with Articles 12, 13 and 14 of the UK GDPR?

Action complete (✓ or ✘)	

The rights of the data subject
All data subjects have rights. Has this been communicated or is information displayed to reflect this, and does it include the: • Right of access • Right to erasure (or right to be forgotten) • Right to data portability • Right to object • Right to rectification • Right to restriction of processing • Right to notification • Right not to be subject to automated decision-making (including profiling)

Action complete (✓ or ✘)	

Subject access requests
All data subjects have a right to access their data and any supplementary information held. Does the practice policy reflect the UK GDPR and do staff understand: • There is no fee applicable for SARs • The response time is one calendar month? • Requests can be refused, but must be fully justified? • Requests can be received by email?

Action complete (✓ or ✘)	

Processing personal data
Do data processors within the practice understand that they are responsible for the processing of data on behalf of the data controller? Do all processors know that one of the following must apply? • The data subject has given consent to the processing of his/her personal data for one or more specific purposes

- Processing is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract

- Processing is necessary for compliance with a legal obligation to which the controller is subject

- Processing is necessary in order to protect the vital interests of the data subject or another natural person

- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller

- Processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child

Action complete (✓ or ✗)	

Consent

• Do current processes for obtaining consent reflect the UK GDPR?
 	
• Do staff know that they must explain to data subjects:
 	
  • Why the organisation wants the data
  • How the data will be used by the organisation
  • The names of any third party data controllers with whom the data will be shared
  • Their right to withdraw consent at any time
 	
• Are staff aware that the Data Protection Act (DPA18) state that parental consent is required for a child under the age of 13; Gillick competence remains unaffected

Action complete (✓ or ✗)	

Data breaches
What are the current procedures to detect and report data breaches? • Do staff know what a data breach is? • What is the reporting process? • Is there a process to notify data subjects of a breach affecting them • How are data breaches recorded; who is responsible for this? • Does the practice policy include data breaches and responsibilities?

Action complete (✓ or ✗)	