GDPR07 - Privacy Notice Policy & Procedure

Category: GDPR **Sub-category:** Policies

Policy Review Sheet

Review Date: 23/05/18 **Policy Last Amended:** 23/05/18

Next planned review in 12 months, or sooner as required.

Note: The full policy change history is available in your online management system.

Business Impact:	Low	Medium	High	Critical
			X	
These changes require action as soon as possible. Changes include fixed implementation dates which are detailed within the policy.				

Reason for this review:	New Policy
Were changes made?	Yes
Summary:	This Privacy Impact Assessment policy will enable organisations to determine when they need to conduct Privacy Impact Assessments. The form included in the policy should be used as a template for each Privacy Impact Assessment.
Relevant Legislation:	• General Data Protection Regulation 2016 • Data Protection Act 2018
Underpinning Knowledge - What have we used to ensure that the policy is current:	• GDPR, (2018), *GDPR Final Text - Articles 35 and 36, Recitals 74-77, 84, 89-92, 94 and 95*. [Online] Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN [Accessed: 04/05/2018]
Suggested action:	• Encourage sharing the policy through the use of the QCS App • Establish process to confirm the understanding of relevant staff • Establish training sessions for staff • Widely distribute the 'Key Facts' of the policy

GDPR07 - Privacy Notice Policy & Procedure

This page is deliberately left blank

GDPR07 - Privacy Notice Policy & Procedure

1. Purpose

1.1 The purpose of this policy is to provide a template privacy impact assessment ("**PIA**") to be used by Wembley Orthodontic Centre on an ongoing basis, as necessary. This policy also explains when a PIA should be conducted.

1.2 Wembley Orthodontic Centre will ensure that the Data Protection Officer will determine when a PIA is required and will complete the PIA, with input as necessary from colleagues and teams.

1.3 To support Wembley Orthodontic Centre in meeting the following Key Lines of Enquiry:

Key Question	Key Line of Enquiry (KLOE)
WELL-LED	HW4: Are there clear responsibilities, roles and systems of accountability to support good governance and management?
WELL-LED	HW5: Are there clear and effective processes for managing risks, issues and performance?

1.4 To meet the legal requirements of the regulated activities that Wembley Orthodontic Centre is registered to provide:

- General Data Protection Regulation 2016
- Data Protection Act 2018

2. Scope

2.1 The following roles may be affected by this policy:

- All staff

2.2 The following people may be affected by this policy:

- Patients

2.3 The following stakeholders may be affected by this policy:

- Family
- Advocates
- Representatives
- Commissioners
- External health professionals
- Local Authority
- NHS

3. Objectives

3.1 The objective of this policy is to ensure that Wembley Orthodontic Centre considers the potential data protection and GDPR implications of any new processes or systems it introduces, or of any changes that impact on its processing of personal data.

3.2 By reviewing and utilising the form set out in this policy, Wembley Orthodontic Centre will be able to provide evidence of the decisions it has taken and changes it has made that may impact on the processing it carries out.

GDPR07 - Privacy Notice Policy & Procedure

4. Policy

4.1 Wembley Orthodontic Centre understands that a PIA will enable it to identify and minimise the risks of any project it wishes to carry out.

4.2 Wembley Orthodontic Centre understands that PIAs must be conducted for specified types of processing (listed in the Procedure section below) as well as for processing that may result in a high risk for affected individuals.

4.3 Wembley Orthodontic Centre understands that a PIA should:

- Describe the nature, scope, context and purposes of the processing
- Assess whether the processing is necessary and proportionate and in compliance with GDPR
- Identify and assess risks to affected Data Subjects; and
- Identify the measures it will take to mitigate those risks

4.4 Wembley Orthodontic Centre understands that if a PIA identifies that processing may be high risk and it is unable to take steps to mitigate those risks, it should notify the ICO and seek advice from the ICO as to whether it should carry out the processing.

GDPR07 - Privacy Notice Policy & Procedure

5. Procedure

5.1 Wembley Orthodontic Centre will implement a process for deciding whether a PIA is necessary and, if so, the steps that it will take to conduct the PIA. Wembley Orthodontic Centre will use the form attached to this policy when conducting a PIA.

5.2 Wembley Orthodontic Centre will provide training to its employees about when a PIA is necessary and how to conduct a PIA.

5.3 Wembley Orthodontic Centre will conduct PIAs in the following scenarios:

- Where Wembley Orthodontic Centre intends to use systematic and extensive profiling or automated decision-making to make significant decisions about Data Subjects
- Where personal data relating to children will be processed for profiling or automated decision making, for marketing to offer online services directly to the children
- Where Wembley Orthodontic Centre will process special categories of data or criminal offence data on a large scale
- Where Wembley Orthodontic Centre intends to monitor a publicly accessible place on a large scale
- Where new technologies are introduced by Wembley Orthodontic Centre that may impact on its processing activities
- Where Wembley Orthodontic Centre intends to process biometric or genetic data
- Where Wembley Orthodontic Centre intends to combine, compare or match personal data from multiple sources
- Where Wembley Orthodontic Centre processes personal data without providing a privacy policy directly to the affected Data Subject
- Where the processing will involve tracking individuals' behaviour (whether online or offline)
- Where the processing could result in a physical harm if there is a breach of security

5.4 Wembley Orthodontic Centre will consider carrying out PIAs in the following circumstances, as well as in any other circumstances which Wembley Orthodontic Centre considers to be potentially high risk:

- Where Wembley Orthodontic Centre processes special categories of data or personal data of a highly personal nature
- Where Wembley Orthodontic Centre conducts large-scale processing; and
- Where the processing concerns vulnerable Data Subjects

Wembley Orthodontic Centre acknowledges that because of the types of services it provides, it may need to conduct PIAs on a regular basis to ensure that Data Subjects, including Patients, are protected.

5.5 Wembley Orthodontic Centre will also conduct a PIA if the nature or purpose of the processing it carries out changes.

5.6 Wembley Orthodontic Centre will document the steps taken as part of the PIA and the outcomes in line with the form attached to this policy.

5.7 Wembley Orthodontic Centre will take any steps it identifies as being necessary to mitigate risks associated with the processing and will document the steps taken and the outcome of those steps.

GDPR07 - Privacy Notice Policy & Procedure

6. Definitions

6.1 Data Subject

- The individual about whom Wembley Orthodontic Centre has collected personal data

6.2 Data Protection Act 2018

- The Data Protection Act 2018 is a United Kingdom Act of Parliament that updates data protection laws in the UK. It sits alongside the General Data Protection Regulation and implements the EU's Law Enforcement Directive

6.3 GDPR

- **General Data Protection Regulation (GDPR)** (EU) 2016/679 is a regulation in EU law on data protection and privacy for all individuals within the European Union. It was adopted on 14 April 2016 and after a two-year trasition period became enforceable on 25 May 2018

6.4 ICO

- The Information Commissioner's Office

6.5 Personal Data

- Any information about a living person including but not limited to names, email addresses, postal addresses, job roles, photographs, CCTV and special categories of data, defined below

6.6 PIA

- A Privacy Impact Assessment, also known as a Data Protection Impact Assessment

6.7 Process or Processing

- Doing anything with personal data, including but not limited to collecting, storing, holding, using, amending or transferring it. You do not need to be doing anything actively with the personal data – at the point you collect it, you are processing it

6.8 Special Categories of Data

- Has an equivalent meaning to “Sensitive Personal Data” under the Data Protection Act 2018. Special categories of data include but are not limited to medical and health records (including information collected as a result of providing health care services) and information about a person’s religious beliefs, ethnic origin and race, sexual orientation and political views

Key Facts - Professionals

Professionals providing this service should be aware of the following:

- All staff should be made aware of how GDPR impacts on their role and ensure that they know who in the Wembley Orthodontic Centre organisation has overall responsibility for data protection
- A PIA is essentially a risk assessment of proposed processing of personal data. If Wembley Orthodontic Centre is processing personal data that is likely to result in a high risk to the Data Subject’s rights, a PIA must be carried out prior to commencing that processing.
- A six-step process maps the lifecycle of the personal data in order to establish: the provenance of the data, the manner of the processing involved, the location of the processing, the relevant stakeholders and the deletion/anonymisation process

GDPR07 - Privacy Notice Policy & Procedure

Key Facts - People Affected by The Service

People affected by this service should be aware of the following:

- PIAs will be conducted by Wembley Orthodontic Centre to ensure that if its processing of personal data changes, any associated risks will be understood and acted upon

Further Reading

There is no further reading for this policy, but we recommend the 'Underpinning Knowledge' section of the review sheet to increase your knowledge and understanding.

Outstanding Practice

To be ‘Outstanding’ in this policy area you could provide evidence that:

- You have implemented a PIA policy and all staff are aware of the potential need to conduct a PIA
- The wide understanding of the policy is enabled by proactive use of the QCS App

Forms

The following forms are included as part of this policy:

Title of form	When would the form be used?	Created by
Privacy Impact Assessment	This form should be used each time an organisation determines that it is necessary to conduct a PIA in line with the guidelines set out in this policy and procedure	QCS

GDPR07 - Privacy Notice Policy & Procedure

This page is deliberately left blank

Privacy Impact Assessment

Annex One: Privacy Impact Assessment Screening Questions	
These questions are intended to help you decide whether a PIA is necessary. Answering 'yes' to any of these questions is an indication that a PIA would be a useful exercise. You can expand on your answers as the project develops if you need to. You can adapt these questions to develop a screening method that fits more closely with the types of project you are likely to assess.	
Will the project involve the collection of new information about individuals?	Y/N
Will the project compel individuals to provide information about themselves?	Y/N
Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	Y/N
Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	Y/N
Does the project involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.	Y/N
Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them?	Y/N
Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be private.	Y/N
Will the project require you to contact individuals in ways that they may find intrusive?	Y/N

Privacy Impact Assessment

Annex Two: Privacy Impact Assessment Template

This template is an example of how you can record the PIA process and results. You can start to fill in details from the beginning of the project, after the screening questions have identified the need for a PIA. The template follows the process that is used in this code of practice. You can adapt the process and this template to produce something that allows your organisation to conduct effective PIAs integrated with your project management processes.

Step one: Identify the need for a PIA

- Explain what the project aims to achieve, what the benefits will be to the Organisation, to individuals and to other parties
- You may find it helpful to link to other relevant documents related to the project, for example, a project proposal
- Also summarise why the need for a PIA was identified (this can draw on your answers to the screening questions)

Privacy Impact Assessment

Step two: Describe the information flows

- You should describe the collection, use and deletion of personal data here and it may also be useful to refer to a flow diagram or another way of explaining data flows. You should also say how many individuals are likely to be affected by the project

Consultation requirements

- Explain what practical steps you will take to ensure that you identify and address privacy risks. Who should be consulted internally and externally? How will you carry out the consultation? You should link this to the relevant stages of your project management process. You can use consultation at any stage of the PIA process

Privacy Impact Assessment

Step three: Identify the privacy and related risks

- Identify the key privacy risks and the associated compliance and corporate risks. Larger-scale PIAs might record this information on a more formal risk register. Annex three can be used to help you identify the DPA related compliance risks

Privacy Issue	Risk to Individuals	Compliance Risk	Associated Organisation/Corporate Risk

Privacy Impact Assessment

Step four: Identify privacy solutions

- Describe the actions you could take to reduce the risks, and any future steps which would be necessary (eg the production of new guidance or future security testing for systems)

Risk	Solution	Result: is the risk eliminated, reduced, or accepted?	Evaluation: is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?

Privacy Impact Assessment

Step five: Sign off and record the PIA outcomes

- Who has approved the privacy risks involved in the project? What solutions need to be implemented?

Risk	Approved Solution	Approved By

Privacy Impact Assessment

Step six: Integrate the PIA outcomes back into the project plan

- Who is responsible for integrating the PIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns that may arise in the future?

Action to be Taken	Date for Completion of Actions	Responsibility for Action

Contact point for future privacy concerns	

Privacy Impact Assessment

Annex Three: Linking the PIA to the Data Protection Principles

Answering these questions during the PIA process will help you to identify where there is a risk that the project will fail to comply with the DPA or other relevant legislation, for example the Human Rights Act

Principle 1

Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:

a) at least one of the conditions in Schedule 2 is met, and

b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met

Have you identified the purpose of the project?	Y/N
How will you tell individuals about the use of their personal data?	
Do you need to amend your privacy notices?	Y/N
Have you established which conditions for processing apply?	Y/N
If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?	
If your organisation is subject to the Human Rights Act, you also need to consider: • 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?	Y/N

Principle 2

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

Does your project plan cover all of the purposes for processing personal data?	Y/N
Have you identified potential new purposes as the scope of the project expands?	Y/N

Privacy Impact Assessment

Principle 3 Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.	
Is the quality of the information good enough for the purposes it is used?	Y/N
Which personal data could you not use, without compromising the needs of the project?	
Principle 5 Personal data processed for any purpose or purposes shall not be kept for longer than necessary for that purpose or those purposes.	
What retention periods are suitable for the personal data you will be processing?	
Are you procuring software that will allow you to delete information in line with your retention periods?	Y/N
Principle 6 Personal data shall be processed in accordance with the rights of data subjects under this Act.	
Will the systems you are putting in place allow you to respond to subject access requests more easily?	Y/N
If the project involves marketing, have you got a procedure for individuals to opt out of their information being used for that purpose?	Y/N
Principle 7 Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data	
Do any new systems provide protection against the security risks you have identified?	Y/N
What training and instructions are necessary to ensure that staff know how to operate a new system securely?	
Principle 8 Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country of territory ensures and adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.	
Will the project require you to transfer data outside of the EEA?	Y/N
If you will be making transfers, how will you ensure that the data is adequately protected?	

Privacy Impact Assessment