Privacy Notice

NEWKIRKGATE DENTAL CARE

We are a Data Controller under the terms of the Data Protection Act 2017 and the requirements of the EU General Data Protection Regulation.

This **Privacy Notice** explains what Personal Data the practice holds, why we hold and process it, who we might share it with, and your rights and freedoms under the Law.

Types of Personal Data

The practice holds personal data in the following categories:

- Patient clinical and health data and correspondence.
- Staff employment data.
- Contractors' data.

Why we process Personal Data (what is the "purpose")

"Process" means we obtain, store, update and archive data.

- Patient data is held for the purpose of providing patients with appropriate, high quality, safe and effective dental care and treatment.
- Staff employment data is held in accordance with Employment, Taxation and Pensions law.
- Contractors' data is held for the purpose of managing their contracts.

What is the Lawful Basis for processing Personal Data?

The Law says we must tell you this:

- We hold patients' data because it is in our **Legitimate Interest** to do so. Without holding the data we cannot work effectively. [Also, we must hold data on NHS care and treatment as it is a **Public Task** required by law].
- We hold staff employment data because it is a **Legal Obligation** for us to do so.
- We hold contractors' data because it is needed to **Fulfil a Contract** with us.

Who might we share your data with?

We can only share data if it is done securely and it is necessary to do so.

- Patient data may be shared with other healthcare professionals who need to be involved in your care (for example if we refer you to a specialist or need laboratory work undertaken). [Patient data may also be stored for back-up purposes with our computer software suppliers] [who may also store it securely] [overseas].
- Employment data will be shared with government agencies such as HMRC.

Your Rights

You have the right to:

- Be informed about the personal data we hold and why we hold it.
- Access a copy of your data that we hold by contacting us directly: we will acknowledge your request and supply a response within one month or sooner.
- Check the information we hold about you is correct and to make corrections if not
- Have your data erased in certain circumstances.

- Transfer your data to someone else if you tell us to do so and it is safe and legal to do so.
- Tell us not to actively process or update your data in certain circumstances.

How long is the Personal Data stored for?

- We will store patient data for as long as we are providing care, treatment or recalling patients for further care. We will archive (that is, store it without further action) for as long as is required for legal purposes as recommended by the NHS or other trusted experts recommend.
- We must store employment data for six years after an employee has left.
- We must store contractors' data for seven years after the contract is ended.

What if you are not happy or wish to raise a concern about our data processing?

You can complain in the first instance to us and we will do our best to resolve the matter. If this fails, you can complain to the Information Commissioner at www.ico.org.uk/concerns or by calling 0303 123 1113.

Legitimate Interest Assessment

For: Newkirkgate Dental Care

Part A: Identifying a Legitimate Interest			
	Question	**Suggested Answer**	**Guidance**
1.	What is the purpose of the processing operation?	For carrying out dental care and treatment of patients	The first stage is to identify a legitimate interest – why is personal data being processed?
2.	Is the processing necessary to meet one or more specific organisational objectives?	Yes – it is a legal and professional requirement	If the processing is required to achieve a lawful business objective then it is likely to be legitimate for the purposes of this assessment
3.	Is the processing necessary to meet one or more specific objectives of any Third Party?	Yes – to conform to General Dental Council Standards and to maintain high professional standards as defined by expert authorities	While you may only need to identify one legitimate interest for the purposes of an LIA – the interest you are seeking to rely on - it may be useful to list all apparent interests in the processing, those of you as the Data Controller as well as those of any Third party who are likely to have a Legitimate Interest (e.g. NHSBSA; HMRC, DWP)
4.	Does the GDPR, ePrivacy Regulation or other national legislation, specifically identify the processing activity as being legitimate, subject to the completion of a balancing test and positive outcome?	Yes – Article 9(2) of the GDPR and Clause 10(2) of the Data Protection Act 2017 refers	An example might be the processing of sensitive personal data in an employee context in which case Article 9(2)(b) of the GDPR is supportive

Part B: The Necessity Test			
	Question	**Suggested Answer**	**Guidance**
1.	Why is the processing activity important to the Data Controller?	To maintain current accurate records of patients' health care and treatment and to identify them for administrative purposes	A Legitimate Interest may be elective or business-critical, however even if the controller's interest in processing personal data for a specific purpose is obvious and legitimate, based on the Controller's objective, it must be clearly articulated and communicated to the individual e.g. in a Privacy Notice
2.	Why the processing activity is important to other parties the data may be disclosed to (if appropriate)?	To ensure the provision of high quality care and treatment to patients as appropriate to their needs; and to ensure the accessibility and accuracy of the records. E.g. dental laboratories and other suppliers, referral practices, clinical data processors (software suppliers) and other expert advisers	A Legitimate Interest may be incidental or business-critical, however the organisation needs to explain clearly what it is. Some purposes may be compelling whilst others may be ancillary. Consider whether your interests relate to a fundamental right, a public interest or another type of interest e.g. the essential safety of the Data Subjects Just because processing is central to the organisation's objectives does not make it legitimate: it is the balance between the organisation's need for

			the processing against the potential impact on the data subject's rights that is key. It is important to consider whose legitimate Interests are being relied on. Understanding this will help inform the context of the processing. In combination with the reason the personal data is being processed, this information will determine the weight of the Legitimate Interest that needs to be balanced.
3.	Is there another way of achieving the objective?	No	If there isn't then clearly the processing is necessary; or If there is another way but it would involve disproportionate effort, then the processing is still necessary: or If there are multiple ways of achieving the objective then a Privacy Impact Assessment should identify the least intrusive means – which would be necessary; or If the processing is not necessary (an unlikely scenario) the Legitimate Interest cannot be relied up on as a lawful basis for that activity

Part C: The Balancing Test			
Question		**Suggested Answer**	**Guidance**
1.	Would the individual expect the processing to take place?	Yes	If individuals would expect the processing to take place, then the impact on the individual is likely to have been already considered by them and accepted. If they have no expectation, then the impact is greater and is given more weight in the balancing test
2.	Does the process add value to a product or service that the individual uses?	Yes	
3.	Is the processing likely to negatively impact the individual's rights?	No	
4.	Would there be a prejudice to the Data Controller if processing did not take place?	Yes	
5.	Is the processing likely to result in unwarranted harm or distress to the individual?	No	
6.	Would there be a prejudice to a Third Party if processing did not happen?	No	

7.	Is the processing in the interests of the individual whose personal data it relates to?	Yes	
8.	Are the legitimate interests of the individual aligned with the party looking to rely on their legitimate interests for processing?	Yes	What are the benefits to the individual or to society? If the processing is of benefit to the individual then it is more likely that Legitimate Interests can be relied upon, as there will be alignment with those of the Controller. Where processing is more closely aligned with the interests of the Controller or a Third Party, than with those of the individual, it is less likely that the interests will be balanced and greater emphasis needs to be placed on the context of the processing and relationship with the individual
9.	What is the connection between the individual and the organisation?	• Existing customer • Lapsed or cancelled customer • Employee or contractor • Business client • Prospective client • Supplier • None of the above	
10.	What is the nature of the data to be processed? Does data of this nature have any special protections under GDPR	• Identification of the individual • Contact details • Current and past health data (Sensitive) • Future clinical care and treatment (Sensitive)	If processing is of special data, and Article 9 condition must be identified as the lawful basis of processing (e.g. specific consent; employment law; vital interests of Data Subject incapable of consenting; provision of lawful health or social care, etc.)
11.	Is there a two-way relationship between the organisation and the individual? How close is that relationship?	e.g. • On-going • Periodic • One-off • None	Where there is an on-going relationship, especially if it is formalised, there would be a greater expectation by the individual that processing will take place.
12.	Would the processing undermine or limit the individual's rights?	No	If processing would undermine or frustrate the future ability to exercise rights that might well affect the balance.
13.	Has the personal data been obtained directly from the individual?	• Yes – in the case of consenting adults • No – in the case of children below the age of consent and vulnerable adults	If information was obtained directly, then due notice should be taken of the notice of fair processing, the relationship with the individual and their expectations of use of their data. If these factors are positive the balance is tipped in favour of the processing operation. If data is obtained indirectly then there may need to be a more compelling Legitimate interest to

			overcome this. The context of the processing and the presence of a two-way relationship may also be relevant
14.	Is there an imbalance in who holds the power between the organisation and the individual?	Yes, however the obtaining of valid consent to care and treatment by each individual or an appointed carer, parent or Attorney validates the processing	Does the individual have a choice regarding the processing of their personal information? If the organisation has a dominant position, this might tip the balance slightly against the use of Legitimate Interests. However the rights and freedoms of individuals as laid down in the GDPR go some way to redressing this issue. The Controller will need to consider how it will address any imbalance of power to ensure that individuals' rights are not impacted
15.	Is it likely that the individual would expect their information to be used for this purpose?	Yes	Given the relationship between the organisation and the individual, including the privacy notices available, would the individual reasonably expect or anticipate that their information would be used for this or a connected purpose? The stronger the expectation the greater the chances that Legitimate Interests can be relied on
16.	Could the processing be considered intrusive or unwarranted? In particular, could it be perceived as such by the individual, or in the context of the relationship?	No. Processing is subject to the requirements of professional confidentiality	Processing should not be unwarranted – intrusion into the private life of the individual may be justified based on the nature of the relationship between the parties or special circumstances. However the greater the perceived intrusion, the more overwhelming the Legitimate Interest must be and the more the rights of the individual considered within the balance
17.	Is a fair processing notice supplied to the individual? If so, how? Is it sufficiently clear and up front regarding the purpose of the processing?	A full Privacy Notice is available on websites, and at the premises and its existence is clearly signposted in all means of contact	The more unusual, unexpected or intrusive the processing, the greater the importance of making the individual aware of the processing, particularly where Legitimate Interests are relied upon
18.	Can the individual whose data is processed control the processing or object to it easily?	Access to clinical records is available to every patient. Records of patients not under continuing or regular care are archived for legal purposes as required by professional authorities	Giving the individual more control over the processing or elements of it may help the Controller rely on Legitimate Interests where otherwise they could not. If individual control is not possible, say why
19.	Can the scope of the processing be modified to reduce or mitigate any underlying privacy risks or	See mitigations in Part D	As with a Data Protection Impact Assessment, a Controller may consider that if there is a privacy risk to the individual, the processing

	harm?		can be limited or adapted to reduce this risk

Part D: Safeguards and Compensating Controls

Safeguards include a range of compensating controls or measures which may be put in place to protect the individual or to reduce any risks or potentially negative impacts of processing. These may have been considered as part of a Privacy Impact Assessment and might include: data minimisation, de-identification, technical and organisational security measures, privacy by design, additional transparency, additional layers of encryption, restricted access, opt-out options.

Add a description of these here:

Examples here would include the use of encryption, secure access to data, details of security applied to any backed-up or stored data off-site, restriction on the use of personal devices for storing or processing data, encryption of e-mails, physical security of the premises. Patients may choose not to opt in to electronic messaging

Part E: Reaching a Decision and Documenting the Outcome

Using the responses above, now document if you believe you are able to rely on Legitimate Interests for the processing operation. Explain, using bullet points why you are, or are not, able to rely on this lawful basis, drawing on the answers provided in this LIA.

Outcome of Assessment:

- Essential for the provision of high quality clinical care and treatment
- Patients would expect processing and storage as a norm
- Professional and legal safeguards for security and accuracy of data apply and are adopted fully
- Care is taken not to undertake unnecessary or excessive processing
- Data is archived according to authoritative guidance for the purpose of legal accountability
- Therefore, I/we believe the Legitimate Interest threshold is met

Signature:		_____
Print Name:		_____
Date:		_____
Role:		_____
Review Date:		_____