

## GDPR Policy and Procedure for Brandhall Dental Care

In May 2018 the EU General Data Protection Regulation (GDPR) replaced the UK Data Protection Act (1998). This policy reflects the changes introduced. All Personnel must ensure they understand the changes and ensure they comply with the principles of GDPR at all times.

To comply with the EU General Data Protection Regulations (GDPR) and the UK Data Protection Act (1998) our Practice has notified the Information Commissioner that personal data and sensitive personal data referring to our Personnel and patients is stored within the Practice.

### 1. INTERPRETATION

#### 1.1 DEFINITIONS:

**We:** means Brandhall Dental Care, 4 Brandhall Road, Oldbury, West Midlands, B68 9AT

**Practice Personnel:** all employees, workers, contractors, agency workers, consultants and others.

**Consent:** agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to them.

**Data Controller:** this is the Practice. The Practice determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the GDPR. We are the Data Controller of all Personal Data relating to our Practice Personnel and Personal Data used in our business for our own commercial purposes.

**Data Subject:** a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

**Data Privacy Impact Assessment (DPIA):** tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving the Processing of Personal Data.

**Data Protection Officer (DPO):** the person required to be appointed in specific circumstances under the GDPR. Where a mandatory DPO has not been appointed, this term means a data protection manager or other voluntary appointment of a DPO or refers to the Practice data privacy team with responsibility for data protection compliance.

**EEA:** the 28 countries in the EU, and Iceland, Liechtenstein and Norway.

**Explicit Consent:** consent which requires a very clear and specific statement (that is, not just action).

**General Data Protection Regulation (GDPR):** the General Data Protection Regulation ((EU) 2016/679). Personal Data is subject to the legal safeguards specified in the GDPR.

**Personal Data:** any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Sensitive Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data is broadly:-

1. Past and present medical and dental condition.
2. Personal details age, NHS number, address, telephone number, email address and the doctor's name and address.
3. Radiographs, clinical photographs and study models.
4. Information about the treatment provided or proposed and it's cost.
5. Notes of conversations/incidents that might occur for which a record needs to be kept.
6. Records of consent to treatment.

8. Any correspondence with other healthcare professionals, i.e. hospital, dental specialists or community services.

**Personal Data Breach:** any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

**Privacy by Design:** implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

**Privacy Guidelines:** guidelines provided to assist in interpreting and implementing this GDPR Policy and Procedure and Related Policies, available [here](#).

**Privacy Notices or Privacy Policies:** separate notices setting out information that may be provided to Data Subjects when the Practice collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals. This is outlined in the Privacy Notice for employees, workers and contractors and a Privacy Notice for Patients.

**Processing or Process:** any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

**Pseudonymisation or Pseudonymised:** replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

**Related Policies:** The Practice policies, operating procedures or processes related to this Policy and Procedure designed to protect Personal Data and also the Privacy Notice for Employees, workers and contractors and the Privacy Notice for Patients.

**Sensitive Personal Data:** information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal Data relating to criminal offences and convictions.

## 2. INTRODUCTION

This GDPR Policy and Procedure sets out how Brandhall Dental Care will handle the Personal Data of our patients, suppliers, employees, workers and other third parties.

This GDPR Policy and Procedure applies to all Personal Data the Practice processes regardless of the media on which that data is stored or whether it relates to past or present employees, workers, patients, clients or supplier contacts, shareholders, website users or any other Data Subject.

## 3. SCOPE

We recognise that the correct and lawful treatment of Personal Data will maintain confidence in the Practice and will provide for successful business operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times. The Practice is exposed to potential fines for failure to comply with the provisions of the GDPR.

All parties are responsible for ensuring all Practice Personnel comply with this GDPR Policy and Procedure and need to implement appropriate Practice processes, controls and training to ensure such compliance.

The DPO is responsible for overseeing this GDPR Policy and Procedure and, as applicable, developing Related Policies and Privacy Guidelines. That post is held by Charlotte South available at Brandhall Dental Care, 4 Brandhall Road, Oldbury, West Midlands, B68 9AT. Please contact the DPO with any questions about the operation of this GDPR Policy and Procedure or the GDPR or if you have any concerns that this GDPR Policy and Procedure is not being or has not been followed.

In particular, you should contact the DPO in the following circumstances:

- (a) if you are unsure of the lawful basis which you are relying on to process Personal Data (including the legitimate interests used by the Practice) (see Section [5.1] below);
- (b) if you need to rely on Consent and/or need to capture Explicit Consent (see Section [5.2] below);
- (c) if you need to draft Privacy Notices or Fair Processing Notices (see Section [5.3] below);
- (d) if you are unsure about the retention period for the Personal Data being Processed (see Section [9] below);
- (e) if you are unsure about what security or other measures you need to implement to protect Personal Data (see Section [10.1] below);
- (f) if there has been a Personal Data Breach (Section [10.2] below);
- (g) if you are unsure on what basis to transfer Personal Data outside the EEA (see Section [11] below);
- (h) if you need any assistance dealing with any rights invoked by a Data Subject (see Section [12] below);

#### 4. PERSONAL DATA PROTECTION PRINCIPLES

We adhere to the principles relating to Processing of Personal Data set out in the GDPR which require Personal Data to be:

- (a) Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency).
- (b) Collected only for specified, explicit and legitimate purposes (Purpose Limitation).
- (c) Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation).
- (d) Accurate and where necessary kept up to date (Accuracy).
- (e) Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation).
- (f) Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality).
- (g) Not transferred to another country without appropriate safeguards being in place (Transfer Limitation).
- (h) Made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).

We are responsible for and are able to demonstrate compliance with the data protection principles listed above (Accountability).

#### 5. LAWFULNESS, FAIRNESS, TRANSPARENCY

##### 5.1 LAWFULNESS AND FAIRNESS

Personal data will be processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

We will only collect, process and share personal data fairly and lawfully and for specified purposes. The GDPR restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Processing but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

The GDPR allows Processing for specific purposes, some of which are set out below:

- (a) the Data Subject has given his or her Consent;
- (b) the Processing is necessary for the performance of a contract with the Data Subject;
- (c) to meet our legal compliance obligations.;
- (d) to protect the Data Subject's vital interests;
- (e) to pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes for which we process Personal Data for legitimate interests need to be set out in applicable Privacy Notices or Fair Processing Notices.

## 5.2 CONSENT

As Data Controller, we will only process Personal Data on the basis of one or more of the lawful bases set out in the GDPR, which include Consent.

A Data Subject consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity will not be sufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

Data Subjects may withdraw Consent to Processing at any time and withdrawal will be promptly honoured. Consent will be refreshed if we intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

## 5.3 TRANSPARENCY (NOTIFYING DATA SUBJECTS)

The GDPR requires Data Controllers to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. Such information will be provided through appropriate Privacy Notices will be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

Whenever we collect Personal Data directly from Data Subjects, including for employment purposes, we will provide the Data Subject with all the information required by the GDPR including the identity of the Data Controller and DPO, how and why we will use, process, disclose, protect and retain that personal data through a Privacy Notice summary which will be presented when the Data Subject first provides the Personal Data.

When Personal Data is collected indirectly (for example, from a third party or publicly available source), we will provide the Data Subject with all the information required by the GDPR as soon as possible after collecting/receiving the data. You will also check that the Personal Data was collected by the third party in accordance with the GDPR and on a basis which contemplates our proposed Processing of that Personal Data.

## 6. PURPOSE LIMITATION

Personal Data will be collected only for specified, explicit and legitimate purposes. It will not be further processed in any manner incompatible with those purposes.

## **We do use cookies on our website –**

A cookie is a small file which asks permission to be placed on your computer's hard drive. Once you agree, the file is added and the cookie helps analyse web traffic or lets you know when you visit a particular site. Cookies allow web applications to respond to you as an individual. The web application can tailor its operations to your needs, likes and dislikes by gathering and remembering information about your preferences.

We use traffic log cookies to identify which pages are being used. This helps us analyse data about web page traffic and improve our website in order to tailor it to our patients' needs. We only use this information for statistical analysis purposes and then the data is removed from the system.

Overall, cookies help us provide you with a better website, by enabling us to monitor which pages you find useful and which you do not. A cookie in no way gives us access to your computer or any information about you, other than the data you choose to share with us.

You can choose to accept or decline cookies. Most web browsers automatically accept cookies, but you can usually modify your browser setting to decline cookies if you prefer. This may prevent you from taking full advantage of the website. Links to other websites – Our website may contain links to other websites of interest. However, once you have used these links to leave our site, you should note that we do not have any control over that other website. Therefore, we cannot be responsible for the protection and privacy of any information which you provide whilst visiting such sites and such sites are not governed by this privacy statement. You should exercise caution and look at the privacy statement applicable to the website in question.

## **7. DATA MINIMISATION**

Personal Data will be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. When Personal Data is no longer needed for specified purposes, it will be deleted or anonymised in accordance with the Company's data retention guidelines.

## **8. ACCURACY**

We will ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. We will check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

## **9. STORAGE LIMITATION**

Personal Data will not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

We will not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

We will maintain retention policies and procedures to ensure Personal Data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time.

We will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with all the Practice's applicable records retention schedules and policies. This includes requiring third parties to delete such data where applicable.

We will ensure Data Subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice or Fair Processing Notice.

## 10. SECURITY INTEGRITY AND CONFIDENTIALITY

### 10.1 PROTECTING PERSONAL DATA

Personal Data will be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

We will implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others and identified risks (including use of encryption and pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data.

We will maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

- (a) Confidentiality means that only people who have a need to know and are authorised to use the Personal Data can access it.
- (b) Integrity means that Personal Data is accurate and suitable for the purpose for which it is processed.
- (c) Availability means that authorised users are able to access the Personal Data when they need it for authorised purposes.

### 10.2 REPORTING A PERSONAL DATA BREACH

The GDPR requires Data Controllers to notify any Personal Data Breach to the applicable regulator and, in certain instances, the Data Subject.

We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.

## 11. TRANSFER LIMITATION

The GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. You transfer Personal Data originating in one country across borders when you transmit, send, view or access that data in or to a different country.

We will only transfer Personal Data outside the EEA if one of the following conditions applies:

- (a) the European Commission has issued a decision confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subjects' rights and freedoms;
- (b) appropriate safeguards are in place such as binding corporate rules (BCR), standard contractual clauses approved by the European Commission, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the DPO;
- (c) the Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or
- (d) the transfer is necessary for one of the other reasons set out in the GDPR including the performance of a contract between us and the Data Subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject where the Data

Subject is physically or legally incapable of giving Consent and, in some limited cases, for our legitimate interest.

## 12. DATA SUBJECT'S RIGHTS AND REQUESTS

Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

- (a) withdraw Consent to Processing at any time;
- (b) receive certain information about the Data Controller's Processing activities;
- (c) request access to their Personal Data that we hold;
- (d) prevent our use of their Personal Data for direct marketing purposes;
- (e) ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;
- (f) restrict processing in specific circumstances;
- (g) challenge processing which has been justified on the basis of our legitimate interests or in the public interest;
- (h) request a copy of an agreement under which Personal Data is transferred outside of the EEA;
- (i) object to decisions based solely on Automated Processing, including profiling (ADM);
- (j) prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;
- (k) be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;
- (l) make a complaint to the supervisory authority; and
- (m) in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine readable format.

We will verify the identity of an individual requesting data under any of the rights listed above

## 13. ACCOUNTABILITY

### 13.1 DATA SECURITY

Under GDPR, the Data Controller must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. The Data Controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.

Brandhall Dental Care has adequate resources and controls in place to ensure and to document GDPR compliance including:

- (a) appointing a suitably qualified DPO (where necessary) and an executive accountable for data privacy;
- (b) implementing Privacy by Design when Processing Personal Data and completing DPIAs where Processing presents a high risk to rights and freedoms of Data Subjects;
- (c) integrating data protection into internal documents including this GDPR Policy and Procedure, Related Policies, Privacy Guidelines, Privacy Notices or Fair Processing Notices;
- (d) regularly training Brandhall Dental Care Personnel on the GDPR, this GDPR Policy and Procedure, Related Policies and Privacy Guidelines and data protection matters including, for example, Data Subject's rights, Consent, legal basis, DPIA and Personal Data Breaches. Brandhall Dental Care will maintain a record of training attendance by Brandhall Dental Care Personnel; and
- (e) regularly testing the privacy measures implemented and conducting periodic reviews and audits

to assess compliance, including using results of testing to demonstrate compliance improvement effort.

### 13.2 RECORD KEEPING

The GDPR requires us to keep full and accurate records of all our data processing activities.

We will keep and maintain accurate corporate records reflecting our processing including records of Data Subjects' Consents and procedures for obtaining Consents in accordance with the Practice's record keeping guidelines.

These records will include, at a minimum, the name and contact details of the Data Controller and the DPO, clear descriptions of the Personal Data types, Data Subject types, Processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place. In order to create such records, data maps should be created which should include the detail set out above together with appropriate data flows.

### 13.3 TRAINING AND AUDIT

We are required to ensure all Brandhall Dental Care Personnel have undergone adequate training to enable them to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.

### 13.4 PRIVACY BY DESIGN AND DATA PROTECTION IMPACT ASSESSMENT (DPIA)

We are required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

We will assess what Privacy by Design measures can be implemented on all programs/systems/processes that Process Personal Data by taking into account the following:

- (a) the state of the art;
- (b) the cost of implementation;
- (c) the nature, scope, context and purposes of processing; and
- (d) the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the Processing.

Data controllers will also conduct DPIAs in respect to high risk Processing.

We will conduct a DPIA when implementing major system or business change programs involving the Processing of Personal Data including:

- (e) use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);
- (f) Automated Processing including profiling and ADM;
- (g) large scale Processing of Sensitive Data; and
- (h) large scale, systematic monitoring of a publicly accessible area.

A DPIA must include:

- (i) a description of the Processing, its purposes and the Data Controller's legitimate interests if appropriate;

- (j) an assessment of the necessity and proportionality of the Processing in relation to its purpose;
- (k) an assessment of the risk to individuals; and
- (l) the risk mitigation measures in place and demonstration of compliance.

### 13.5 DIRECT MARKETING

We are subject to certain rules and privacy laws when marketing to our customers.

For example, a Data Subject's prior consent is required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing customers known as "soft opt in" allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information.

A Data Subject's objection to direct marketing will be promptly honoured. If a customer opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

### 13.6 SHARING PERSONAL DATA

Generally, we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

We will only share the Personal Data we hold with another patient, employee or agent if the recipient has a 'need to know' basis for the information and the transfer complies with any applicable cross-border transfer restrictions.

We will only share the Personal Data we hold with third parties, such as our service providers if:

- (a) they have a need to know the information for the purposes of providing the contracted services;
- (b) sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;
- (c) the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
- (d) the transfer complies with any applicable cross border transfer restrictions; and
- (e) a fully executed written contract that contains GDPR approved third party clauses has been obtained.

### 14. CHANGES TO THIS GDPR POLICY AND PROCEDURE

We reserve the right to change this GDPR Policy and Procedure at any time without notice to you, so please check back regularly to obtain the latest copy of this GDPR Policy and Procedure