**Information**

**Governance**

This document and its content is produced solely and exclusively for the use of member dentists offering Denplan payment plans and their authorised practice staff who are permitted to download, print and amend to suit their personal circumstances and for use in their own practice(s) only.

**© 2022 DENPLAN LTD | ALL RIGHTS RESERVED**

Copyright in the whole and every part of this manual belongs to Denplan Limited and may not, other than in strict accordance with the terms above, be used, sold, transferred, copied or reproduced in whole or in part in any manner or form or in or on any media to any other person without the prior written consent of Denplan Ltd.

Updates are highlighted in yellow

**Content Review Due June 2023**

**Contents**

[Introduction 4](#Page_4)

[Data Protection in Dental Practice 5](#Page_5)

[Points to note about the Data Protection Act 2018 and the GDPR 7](#Page_7)

[Data Protection Policy 9](#Page_9)

[Legitimate Interest Assessment 12](#Page_12)

[Notes to the Privacy Notices Templates for Dental Practices 19](#Page_19)

[Privacy Notices for Patients 20](#Page_20)

[Privacy Notices for Workers 24](#Page_24)

[Data Protection Breach Notification form 29](#Page_29)

[Accidental Disclosure of Confidential Information 32](#Page_32)

[Data Audit Template Notes 34](#Page_34)

[Data Audit 35](#Page_35)

[Guidance on Retention of Records in Dental Practice 38](#Page_38)

[Data Retention Schedule 41](#Page_41)

[Cookies Policy 43](#Page_43)

[Cookie Policy Template 45](#Page_45)

[Information Security 47](#Page_47)

[Information Security Policy 49](#Page_49)

[Data Protection Policy Statement 53](#Page_53)

[Social Media 55](#Page_55)

**Introduction**

The General Data protection Regulations (GDPR) were adopted and issued by the EU in May 2016, giving all Member States two year to comply. The new Data Protection Act 2018 incorporated the new provisions of GDPR and this came into force on 25th May 2018.

Whilst dental practices will already be conversant with the requirements and significance of the Data Protection Act 1998, this new Legislation introduced some changes that data controllers should have adopted. The Information Commissioner’s Office, (ICO), have issued a “12-step Guide” to the GDPR which should be followed as a starting point.

The resources available within this manual are designed to support you in complying with the requirements of the new Act and are tailored towards the needs of primary dental care practices. This document and its content, are produced solely and exclusively for the use of member dentists and their authorised practice staff who are permitted to download, print and amend to suit their personal circumstances and for use in their own practice(s) only. Whilst it is believed that these documents are a reasonable interpretation of the requirements of all relevant legislation and are produced in good faith, Denplan Limited (trading as Simplyhealth Professionals) has no liability for any errors or admissions. It is your responsibility to check and ensure that any documents adapted and used by you meet your own specific practice needs.

Further guidance should be obtained from the Information Commissioner’s Office website at: <https://ico.org.uk/>

The Data Protection Network also publishes views, analysis, generic practical resources and supportive guides, developed and edited by data protection specialists. The website is: <https://www.dpnetwork.org.uk/founding-partners/>

**Data Protection in Dental Practice**

On the 25th Of May 2018 the Data Protection Act 1998 was superseded by the EU General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA18). This significantly extends the former Act in line with global advances in digital data processing, and affects all organisations, including dental practices.

Dentists must also observe: the General Dental Council’s Standards (4.1 to 4.5); the Access to Health Records Act 1990 (AHR); the Privacy and Electronic Communications Regulations 2011 (PECR); and (for NHS contract holders) the Freedom of Information Act 2000 (FOIA).

**The GDPR and DPA18** requires that all Data Controllers must (see [www.ico.org.uk](http://www.ico.org.uk)):

* Process data which can directly or indirectly identify a living individual in accordance with the law and have a Policy for so doing
* Have a Lawful Basis for such processing
* Publish to Data Subjects a Privacy Notice setting out the scope of processing and Subjects’ rights
* Have a process to allow Data Subjects to access their data within a set timeframe, and without charge
* Hold and process data securely and set out retention periods
* Register with the Information Commissioner and pay a fee

**The GDC** requires (see: [www.gdc-uk.org/professionals/standards](http://www.gdc-uk.org/professionals/standards)) all registrants to:

* Maintain complete, clear, accurate and current patient records
* Keep all patient details confidential
* Permit patients to access their records
* Store records securely

**The Access to Health Records ACT 1990 (AHR)** requires:

* That patients have access to their health records and…
* …this right extends to the representatives of a deceased patient

**The Privacy and Electronic Communications Regulations (PECR)** require (see: https://ico.org.uk/for-organisations/guide-to-pecr/) that:

* Consent is obtained to communicate for marketing purposes via electronic means (e-mail, telephone, SMS or similar)
* Recipients must be advised of, and consent to, information placed on their devices (“cookies”)

**The Freedom of Information Act 2000 (FOIA) (and equivalent Scottish law)** requires (see: https://www.legislation.gov.uk/ukpga/2000/36/contents) that:

* Public Authorities (including NHS dental practices) must have a Publication Scheme
* The public may request to access the information contained in that Scheme

**Points to note about the Data Protection Act 2018 and the GDPR**

In addition to specifying what constitutes Personal Data, GDPR also identifies “special categories” of data including race/ethnicity, health, genetic, biometric and sexual. Schedule 1, Part 1 of DPA18 permits processing of special data for health or social care purposes, conducted by a health professional.

Data may not be transferred outside the EU unless the transfer is subject to adequate safeguards. Where a Data Processor, such as a software company, holds or backs up data outside the EU this must be contractually documented as to safeguards and compatibility with EU data protection law (e.g. Privacy Shield in the US).

Unless a data access request can be shown to be manifestly unfounded or excessive, no charge can be made to the Data Subject and a response within one month is required (extendable if very complex).

The Data Protection principles in the GDPR (Article 5) are that data shall be:

* Processed lawfully, fairly and in a transparent manner
* Collected for specified, explicit and legitimate purposes
* Adequate, relevant and necessary
* Accurate and updated
* Kept for no longer than is necessary
* Processed in a secure manner and protected against loss, destruction or damage

Data Subjects have the following rights under GDPR:

* To be informed of processing, its purpose, origin and any disclosure
* To access their information on request
* To have erroneous data corrected
* To have their data erased (in certain circumstances)\*
* To restrict processing of their data (with some exceptions)\*
* To have their data sent to another data controller (in certain circumstances)\*
* To object to their data being processed (unless there are compelling grounds)\*
* To object to automated processing (unlikely in dental practices)

\**It is unlikely that such circumstances would arise in a healthcare setting: in such cases advice should be sought from the Information Commissioner or your professional indemnity provider.*

Public Authorities including NHS contract-holding dentists/practices, are required to appoint a Data Protection Officer. Under the GDPR this cannot be the Data Controller and must be a person who is independent, an expert in data protection, and reporting to top management. It can be an employee or an external appointment.

An annual fee (subject to parliament) is payable to the Information Commissioner (ICO) by Data Controllers. The fee (payable on first registration or the anniversary of any existing notification) is:

* £40 if your turnover is less than £632,000 or you have no more than 10 staff\*
* £60 if your turnover is less than £36 million or no more than 250 staff. (Fees are reduced by £5 if paid by direct debit)

\*Staff includes part-time workers, employees or office-holders. For NHS practices, only the staff limit applies (not the turnover limit).

**Data Protection and Self-employed Associates**

Although most associates are self-employed, their individual circumstances will dictate whether they are a Data Controller or a Data Processor. If they are a Data Controller, they will need to register, pay the ICO fee and fully comply with DPA18 and GDPR.

If, however, control of the data in the practice is in the hands of the practice owner/s and the Associate is only processing it under direction and in accordance with practice policies they may not be considered to “own” the data. The Information Commissioner has produced guidance on this: see [www.ico.org.uk](http://www.ico.org.uk) and search “*Information Governance in Dental Practices” Sept 2015.*

**Access to Health Records Act 1990**

In general, the release of records to a patient on their personal request will be handled under the Data Protection Act. However, should you be approached by a deceased patient’s representative, their advisors or other third parties or officials, you should contact your professional indemnity provider for advice.

**Freedom of Information Act 2000**

Dentists holding an NHS contract can find information about compliance with the FOIA and a model publication scheme from the ICO: <https://ico.org.uk/for-organisations/guide-to-freedom-of-information/publication-scheme/> and can find a model scheme for NHS dental practices at: https://ico.org.uk/media/for-organisations/documents/1276/dentists\_guidance.doc

In Scotland, details of the Freedom of Information (Scotland) Act 2002 can be obtained from: [www.itspublicknowledge.info](http://www.itspublicknowledge.info)

**Data Protection Policy**

Oak House Dental Practice

1. **General**

The practice collects, holds, processes and shares personal data in accordance with the provisions of the General Data Protection Regulation and the Data Protection Act 2018. We have carried out and will review as appropriate, a Data Audit.

This Policy applies to personal data in the following categories:

* Patients’ Records, both current and past
* Employees’ data
* Contractors’ data - including dental registrants
* CCTV footage

1. **Data Protection Principles**

We shall ensure that Personal Data, including Special Data (health) will be:

* Processed lawfully, fairly and in a transparent manner
* Collected for specified, explicit and legitimate purposes only
* Adequate, relevant and necessary for the purpose
* Accurate and updated
* Kept for no longer than is necessary
* Processed in a secure manner and protected against loss, destruction or damage

1. **Lawful Basis**

Data will be held and processed under the following Lawful Basis:

* Patient Data and health records: for the Legitimate Interests of the practice in providing health care and treatment
* Employment records: as a Legal Obligation for the provision of Employment Terms and conditions and supply of data to HM Revenue and Customs and other statutory functions such as pensions and benefits.
* Contractor Data: for the fulfilment of contracts.
* CCTV Data: for the detection and prevention of crime

We will additionally secure the specific consent of patients for the provision of electronic communication under the Privacy and Electronic Communication Regulations 2011

1. **Data Subjects’ Rights**

We will ensure that the rights of Data Subjects are respected and maintained by:

* The issue and promotion of a Privacy Notice detailing data processed, its origin and any disclosures, the Lawful Bases for processing, and the rights of Data Subjects
* The maintenance of a Subject Access process and the appointment of Andrew Ridout as Data Protection Officer to oversee that process and to advise on compliance.
* A legitimate interest assessment ensuring individuals’ rights are balanced with the legitimate needs of the practice.
* A Data Retention schedule.
* An Information Security policy.
* A Data Breach Policy.
* Contractual assurance of adequate safeguards if data is processed outside the European Union.

1. **Subject Access Requests**

All data subjects may submit a request to be informed of the data we hold about them, its lawful basis and from whom it is/was obtained and to whom it may be disclosed. We will provide this information without charge and as soon as is reasonably possible and in any event within one month of a valid request being received. Access requests should be addressed (or forwarded without delay) to Andrew Ridout.

1. **Training and Compliance**

We will ensure that all staff are aware of their duty of strict confidentiality regarding personal data, both professional and under the Data Protection law. We will provide training and assure compliance and will review and refresh training on a regular basis.

It is a condition of continuing employment that all staff are aware of, sign their acceptance of, and comply with, their obligations under this Policy. Any queries or concerns must be immediately addressed to Andrew Ridout. A breach of this Policy may amount to misconduct and result in disciplinary action. Serious or persistent breaches may result in dismissal.

1. **Security of Data**

The practice will publish and maintain an Information Security policy to assure against any loss, damage, unlawful disclosure or non-compliant erasure of data. All staff will be trained and advised of their obligations under this Policy.

**Legitimate Interest Assessmen**[**t**](#Page_12)

Under the data protection Act 2018 personal data must be processed lawfully. Some data processing is necessary for legal reasons such as payroll information. Where there is no legal reason, data can still be processed if there is a legitimate interest in doing so.

**For:** Oak House Dental Practice

|  |  |  |  |
| --- | --- | --- | --- |
| Part A: Identifying a Legitimate Interest | | | |
| Question | | 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 2018 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 | | 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 | | 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. |  | 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 harm? | 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 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:**

|  |
| --- |
| All data is protected by double password protection, as well as being encrypted and stored securely.  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: |  | Andy Ridout |
| Print Name: |  | Andrew Ridout |
| Date: |  | 12/02/2023 |
| Role: |  | Principle Dentist |
| Review Date: |  | February 2024 |

**Notes to the Privacy Notices Templates for Dental Practices**

***Important****: Text in italics MUST be redacted from the following documents before they are issued by a dental practice. The Information Commissioner has indicated that Privacy Notices must be written clearly, transparently and accessibly. Avoid complex language wherever possible.*

*It is also essential that a practice’s Privacy Notices accurately reflect its individual circumstances. Therefore, a Data Audit must be completed before the final wording is completed so that all types of data, sources of data and data disclosures are identified and included.*

*Text in square brackets […] but* not *in italics indicates possible alternatives (which are not exclusive). In these cases, the appropriate alternative should be inserted and the brackets deleted.*

*These document are updated versions of those issued in April 2018 in the light of the Information Commissioner’s recommendation that Privacy Notices should be specific to the data subject (e.g. patients, staff, contractors, etc.).*

***Data Erasure Right:*** *The law requires you to tell Data Subjects about this right, but there are a number of compelling and legitimate reasons not to grant this request. See:* [*www.ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure*](http://www.ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure)

*The left-hand tabs on the above web page also provide more detail about the circumstances in which Data Subjects can, and cannot, exercise the other Rights listed in these Privacy Notices.*

*As always, this information is provided as guidance and is not mandatory or exclusive. In case of doubt, you should always consider taking further advice either from the Information Commissioner’s website at* [*www.ico.org.uk*](http://www.ico.org.uk) *or from an appropriate authority.*

It is clearly impractical for the full information in a Privacy Notice to be conveyed to every Data Subject or potential Data Subject at their first contact. However, its existence must be clearly signposted and a copy readily available and accessible (e.g. in print, in Practice Manuals, and for patients, on a website page).

Additionally, staff manuals, websites and any printed material which is made available to patients, workers and prospective workers at their first contact (or, for patients, at recall) such as a Medical History questionnaire or Practice Information Leaflet contains wording such as:

|  |
| --- |
| At the ……………………….. Dental Practice, we take great care with all the Personal Information we hold, to ensure we comply with best professional practice and with the law. For a full copy of our Data Privacy Notice, please [click here]; [ask at Reception]; [ask any member of staff]; [see our Noticeboard]; [read our Patient Information Leaflet] |

**Privacy Notice for Patients**

Oak House Dental Practice

We are a Data Controller under the terms of the Data Protection Act 2018. We are registered with the Information Commissioner No: *Z5861079*

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

|  |  |
| --- | --- |
| Our Contact Details | |
| Practice name and address: | *Oak House Dental Practice 13 St. Georges Road, Truro TR1 3JE* |
| Practice telephone number(s): | *01872 222922* |
| Practice e-mail address: | [*theteam@the-oak-house.com*](mailto:theteam@the-oak-house.com) |
| Practice website: | [*https://the-oak-house.com*](https://the-oak-house.com) |
| Person responsible for Data Protection queries: | *Andrew Ridout* |

**What types of patients’ Personal Information do we hold?**

The practice holds patients’ Personal Information in the following categories:

* Name, identity, (e.g. date of birth) and contact details.
* Family details including anyone who may need to give consent for your care.
* Medical history, your GP’s details, [your NHS number]
* Dental history, records of treatment provided, x-rays and photographs.
* Information from other providers involved in your care.
* Dates of you appointments including any that are cancelled or that you have not attended.
* Payment details and financial information in connection with your care.
* Correspondence relating to your care with you or with other healthcare professionals.
* Details of any complaints that you have made and how we dealt with them.

**Why do we process patients’ Personal Information? (What is the “purpose”?)**

“Process” means we obtain, store, update and archive your Information.

Patients’ Personal Information is held for the purpose of providing patients with appropriate, high quality, safe and effective dental care and treatment and the maintenance of accurate records.

**Other reasons for storing your information:**

* **Research or educational purposes**

We may also use your information for research or educational purposes. If we wish to do this we will discuss the details with you and seek your consent. Whenever possible this information will be anonymised.

* **Direct Marketing**

We may use your contact details to inform you of products and services available at the practice. If you would like to opt out of this, please inform reception.

* **CCTV**

We have CCTV at the practice for [patient and staff safety] *amend as applicable* [please see our CCTV policy]

**What is the Lawful Basis for processing your Personal Information?**

The Law says we must tell you this.

We hold patients’ Personal Information because it is in our **Legitimate Interest** to do so. Without holding the Information we cannot provide your care and treatment effectively.

**What do we do with your Information?**

We will only share your information if it is done securely and it is necessary for us to do so.

* Your personal information may be securely shared with other healthcare professionals who need to be involved in your care (for example if we refer you to a specialist, need laboratory work undertaken or need to consult with your doctor)
* There may be times when we are need to disclose relevant information to third parties not involved in your care for example:
* A debt collection agency (if fees owing remain unpaid)
* HMRC.
* Other Law inforcement or government agencies.
* We may also share your personal information securely to third parties where we are required by law or regulation to do so. This may include:
  + The General Dental Council
  + The Care Quality Commission *[or relevant Regulatory body]*
  + Dental payment plans or insurers

**How do we store your Information?**

Your Information is stored securely at the practice [in paper form] [and on protected computer systems]. Computer information is backed up regularly and may be securely stored away from our premises.

We will keep your Information for as long as you are having dental care and treatment from us or ask us to remind you or send you future appointments. Otherwise we will archive it (that is, store your Information without processing it. For fifteen years from your last contact with us (or until you are age 25 if you are 16 and under, or age 26, if aged 17 when treatment finished.

**What are your data protection rights?**

Under data protection law you have the right to:

* Be informed about the personal information we hold and why we hold it.
* Have 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, without charge.
* Check the information we hold about you is correct and if not to make corrections.
* Have some of your data erased in certain circumstances.
* Transfer your information 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 information in certain circumstances.

**What if you are not happy or wish to raise a concern about our processing of your Information?**

You can complain in the first instance to our Data Protection Officer, who is *Andrew Ridout* [*denplandentist@btconnect.com*](mailto:denplandentist@btconnect.com)and we will do our best to resolve the matter.

If you do not agreeto the use of your information as described, it may not be possible for us to continue to provide your dental care.

|  |
| --- |
| If this fails, you can complain to the Information Commissioner at:   * [www.ico.org.uk/concerns](http://www.ico.org.uk/concerns), by calling 0303 123 1113, or by writing to: The Information Commissioner’s Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF |

**Privacy Notice for Workers**

Oak House Dental Practice

We are a Data Controller under the terms of the Data Protection Act 2018. We are registered with the Information Commissioner No: *Z5861079*

This **Privacy Notice** explains what Personal Information relating to Workers the practice may hold, why we hold and process it, who we might share it with, and your rights and freedoms under the Law.

**Who are considered Workers?**

* The term ‘Workers’ as defined within the Information Commissioner’s Employment Practices Code includes current and former:
* Job applicants (successful or not)
* Employees
* Agency Staff
* Casual Staff
* Contract Staff (including self-employed registered dental professionals)
* Volunteers
* Work Placement individuals

|  |  |
| --- | --- |
| Our Contact Details | |
| Practice name and address: | *Oak House Dental Practice 13 St. Georges Road, Truro TR1 3JE* |
| Practice telephone number(s): | *01872 222922* |
| Practice e-mail address: | [*theteam@the-oak-house.com*](mailto:theteam@the-oak-house.com) |
| Practice website: | [*https://the-oak-house.com*](https://the-oak-house.com) |
| Person responsible for Data Protection queries: | *Andrew Ridout* |

**What types of Workers’ Personal Information do we hold?**

The practice may hold personal data in the following categories (where it is necessary and relevant to your work):

* Name, proof of identity, date of birth and contact details.
* Contracts of employment (employees) or engagement.(self employed workers eg. Associates. (and any amendments)
* Relevant and updated health(including immunisation records and conditions that may affect your ability to work or that require us to provide support and assistance) and employment history, training and qualifications.
* Information regarding safeguarding. (e.g. DBS checks)
* Information regarding professional registration and professional indemnity.
* References
* Appraisals, performance and monitoring records. (employees)
* Sickness, injury, absence and accident records.
* Disciplinary, grievance and dismissal records. (employees)
* Financial, banking, Tax and National Insurance information and records.
* Correspondance with you and relevant third parties regarding your employment at the practice.
* Clinical Audits relating to your work at the practice. (Associates)
* Issues or feedback received in relation to your work at the practice.(Associates)

**Why do we process Personal Information? (What is the “purpose”?)**

“Process” means we obtain, store, update and archive your Information.

Workers’ Personal Information is held for the purpose of managing an efficient, well-regulated and ethical practice providing quality dental care and a good working environment, and for the fulfilment of the practice’s legal and regulatory obligations.

We have CCTV at the practice for patient and staff safety, please see our CCTV policy

**What is the Lawful Basis for processing your Personal Information?**

The Law says we must tell you this.

We hold Job Applicants’, Volunteers and Work Experience individuals’ Personal Information for our necessary **Legitimate Interests** in order to fulfil our purpose as above.

We hold Employees’ Personal Information because it is a **Legal Obligation** to do so. For instance, we must comply with the Employment Act (2018), the Dentists Act (1984), the Health and Safety At Work Act (1974), the Health and Social Care Act (2012), the National Health Service act (1977) and the Finance Acts.

We hold Contractors’ Personal Information because it is required to fulfil a **Contract** between them and the practice.

**What do we do with your Information?**

We will only share your information if it is done securely and it is necessary and relevant, or required by law, for us to do so.

For instance, we may share information under those conditions with:

* HM Revenue and Customs.
* The Care Quality Commission.
* The General Dental Council.
* Health and Safety Executive.
* Department for Work and Pensions.
* Pensions providers.
* Training providers.
* Professional Advisers such as accountants, lawyers, indemnity providers.
* Dental plan providers and insurers.
* Locum agencies.
* New or prospective practice owner. (in accordance with TUPE regulations)
* If you leave the practice and find another job we may provide a reference for you to the new of prospective employer (at your request)

Information shared will be the minimum necessary.

**How do we store your Information?**

Your Information is stored securely at the practice [in paper form] [and on protected computer systems]. Computer information is backed up regularly and may be securely stored away from our premises.

* We will keep personal information for unsuccessful Job Applicants for no longer than six months after the completion of the relevant recruitment process unless they explicitly request otherwise.
* We will keep personal information for volunteers and work placement individuals for no longer than six months after the completion of their engagement with us unless they explicitly request otherwise.
* We will keep personal information for employees and contractors for the period of their employment or contract with the practice and on termination of that employment or contract (or of any matter arising from it) we will archive their records (that is, securely store them without further processing) for six years after which time they will be securely destroyed and/or erased.

**What are your Data Protection rights?**

Under data protection law you have the right to:

* Be informed about the personal information we hold and why we hold it.
* Have 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, without charge.
* Check the information we hold about you is correct and if not to make corrections.
* Have your data erased in certain circumstances. (but not if it is held as a Legal Obligation)
* Tell us not to actively process or update your information in certain circumstances.
* Request that we stop using your information for some non-essential purposes.

**What if you are not happy or wish to raise a concern about our processing of your Information?**

You can complain in the first instance to our Data Protection Officer, who Andrew Ridout [denplandentist@btconnect.com](mailto:denplandentist@btconnect.com) 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](http://www.ico.org.uk/concerns), by calling 0303 123 1113, or by writing to: The Information Commissioner’s Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF |

**Data Protection Breach Notification Form**

**ICO Registration Number (if known):** *Z5861079*

Mandatory details (\*)

|  |  |  |  |
| --- | --- | --- | --- |
| Section 1: Notification of Breach | | | |
| 1.\* | Date and time incident was discovered |  | Act as soon as reasonably practical: individual reporting incident to complete |
| 2.\* | Date incident occurred if different to above |  |  |
| 3. | Location of incident |  | e.g. on business premises, at home, in car, etc. |
| 4. | Name of individual reporting incident |  |  |
| 5. | Contact details of individual reporting incident (e-mail & phone) |  |  |
| 6.\* | Description of incident and details of lost data |  | How did the breach occur?  Did the data refer to identifiable living individuals? |
| 7.\* | Number of data subjects affected if known or approximate |  |  |
| 8. | Brief description of any immediate action taken when discovered |  | e.g. incorrectly addressed e-mail deleted by recipients; data subject advised, etc. |

|  |  |  |  |
| --- | --- | --- | --- |
| Section 2: Severity Assessment | | | |
| 9. | Details of IT system/s, equipment, devices and/or data records involved in the breach |  | Give as much detail as possible |
| 10. | What information was lost? |  | Brief description of the category e.g. clinical records, employment data |
| 11.\* | What is the nature of the information? |  | e.g. health data, personal records, financial details |
| 12. | How much data has been lost? |  | Estimate file sizes, number of records etc. Were entire systems affected? |
| 13.\* | Is the information retrievable or replaceable? |  | Was the data effectively backed up? When? Has it been checked? How old is the back-up? |
| 14. | How many data subjects are involved? |  | E.g. number of patients, employees affected? |
| 15. | Was the data encrypted? |  | Details of encryption system used if available |

|  |  |  |  |
| --- | --- | --- | --- |
| 16.\* | Is the data sensitive?(GDPR: special under Article 9) |  | Does data concern health, race or ethnicity, politics or religion |
| 17.\* | Do the data subjects include children (<18 years) or vulnerable adults |  | If so specify approximate numbers or percentages |
| 18. | Does the data include information that could facilitate identity theft? |  | Does the data include banking details, NI numbers, photocopies of passports or similar |
| 19.\* | Does data include information which could cause significant distress or damage? |  | e.g. details of performance, disciplinary action, or personal lifestyle |
| 20. | Does the information contain security data which might compromise the safety of individuals? |  | e.g. Access codes, confidential address data, etc. |

|  |  |  |  |
| --- | --- | --- | --- |
| Section 2: Action Taken (for completion by Data Protection Officer) | | | |
| 21.\* | Name of Data Protection Officer |  | Include contact details if reporting to ICO |
| 22. | Date and time of receipt of report |  |  |
| 23. | Immediate action taken |  | e.g. Back-up checked or requested, passwords changed, IT company contacted |
| 24. | Police notified? | * Y/N * Crime number * Badge number/name of Officer/contact * Force me or contact details | e.g. theft of laptop, computer or device, malicious cyber-activity or other criminal action |
| 25. | ICO Notified? | * Y/N * Date and time of notification | Include name of organisation and registration No. if known plus all mandatory details (\*), and any previous incidents |
| 26. | Other external stakeholders or regulators notified |  | e.g. CQC or similar regulator  legal advice sought; IT or technical advice sought |
| 27. | Other actions taken by Principals/Data Protection Officer |  |  |
| 28.\* | Have affected Data Subjects been notified of loss or theft? | Y/N | Give reason(s) for action taken or proposed |
| 29. | Further Action recommended |  |  |

|  |  |  |
| --- | --- | --- |
| **Signature of person reporting breach:** |  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **Print Name:** |  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **Date:** |  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

|  |  |  |
| --- | --- | --- |
| **Signature of Data Protection Officer:** |  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **Print Name:** |  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **Date:** |  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

Note: if the data breach includes information which:

* could cause significant distress or damage to individuals, or
* could compromise the safety of individuals, especially children or vulnerable adults, or
* is of a volume or nature which may cause serious reputational damage.

Then consideration should be given to notifying the ICO and also taking advice from expert external sources.

Reports to the Information Commissioner should be made within 72 hours to [casework@ico.org.uk](mailto:casework@ico.org.uk) with ‘DPA Breach Notification form’ in the subject field. Further information can be found at: [www.ico.org.uk/](http://www.ico.org.uk/) - search ‘Personal data breaches’.

This record should be kept even if no adverse consequences are anticipated or notifications are required.

**Accidental Disclosure of Confidential Information**

Oak House Dental Practice

At Oak House Dental Practice we are aware of Article 5 (1) (f) of the General Data Protection Regulation which states that personal data shall be:

|  |
| --- |
| “…protected against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures”. |

If a Data Breach occurs, we would take the following steps:

1. Containment and recovery.
2. Assessment of ongoing risk.
3. Notification of breach.
4. Evaluation and response.

**Containment and Recovery**

As soon as a data breach is discovered, we would assign a person to be responsible for ensuring that the breach is documented using our Data Breach template, and contained. We would establish who needs to be aware of the breach and how they can help in containing it. This may involve shutting down computer systems or establishing new access codes, finding new safe storage for record cards, or changing locks on doors.

We would act to recover any lost or corrupted data as soon as possible <using back up tapes/restoring lost or damaged data from off-site back up>.

**Assessment of Ongoing Risk**

We would access the type of data involved and its level of sensitivity. We would also assess how much data was involved and the number of people affected.

We would endeavour to find out what has happened to the data and if stolen, whether it could be used harmfully. We would assess whether the data could lead to physical risk, significant distress or damage for the people involved. We would also assess whether the information could lead to identity fraud or financial loss.

Dependent on the type of data we would also assess the damage to the reputation of the practice.

**Notification of Breach**

We would decide who needed to be informed of the breach. This would be based on who was involved and the type of information. We would make sure that we were meeting our security obligations with regard to the principles set out in Article 5 of the GDPR. We would also make sure we have a clear purpose as to our reasons for notifying affected individuals.

If we felt it was appropriate in that:

* The volume or nature of data loss was significant.
* The data related to children or vulnerable persons.
* The data was likely to cause significant distress or damage to individuals.
* The data was likely to incur significant reputational damage to the practice.

- Then we would consider making notification as appropriate to:

* The Information Commissioner. (within 72 hours of discovery)
* Healthcare regulator.
* NHS authorities.

We would discuss with our defence organisation how we should inform the people affected by the breach and what we should say to them. We would make sure we had a contact point in the practice for anybody who had queries to be able to contact.

If it was felt necessary we would inform the ICO. For guidance on whether to inform them we would go to [www.ico.org.uk](http://www.ico.org.uk)

**Evaluation and Response**

We would investigate the cause of the breach and how we responded to it. We would review all aspects and update our policies and procedures in light of what we found.

We would ensure that our Data Breach template was completed for every breach, no matter how apparently slight or insignificant, so that we could learn from every issue and take appropriate corrective action for the future.

We would look for any weak points in our system and work to improve them. This may involve further training of staff, assignation of responsibilities and ongoing monitoring.

**Data Audit Template**

*Explanatory Notes*

In advance of the introduction of a new Data Protection Act and the EU General Data Protection Regulation (GDPR) on 25th May 2018, the Information Commissioner’s Office (ICO) has recommended that, as an initial step, all Data Controllers should carry out an audit of the data flows within their organisation. (See [www.ico.org.uk](http://www.ico.org.uk)).

A Data Audit is not compulsory but demonstrates that you have considered all the Personal Data\* that is applicable in your practice, whether it is processed\*\* in paper format or electronically, and by you and your team or a third-party Data Processor such as a practice management software company.

Note that data processing (even if the data is only “held”, backed-up or archived) by a third party such as a software company, must be evidenced by a written contract specifying the location (country, and whether outside the European Economic Area), security measures in place, and compliance with the GDPR.

The following template sets out the kind of data that it might be anticipated that a dental practice would hold. Please note, however that it is not designed to be exhaustive nor mandatory. It is important that *your* Data Audit is reflective of *your* practice’s actual profile.

*In particular, ensure that when you have completed the fields (adding or removing those that reflect your situation), you delete all the notes in square brackets (and these explanatory notes).*

The Data Protection Act and GDPR apply to all parts of the UK and your documentation may be inspected by Healthcare Regulators and, if you are an NHS contract holder, the relevant commissioning Authority.

\*Personal Data is data which does or could relate to an identifiable living individual, either directly (e.g. by name, address, etc.), *or* indirectly (e.g. a registration number, NHS number).

\*\*Processing includes collecting, storing, entering, amending, updating, disclosing, sharing, archiving or destroying Personal Data.

**Data Audit**

Oak House Dental Practice

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Business Function | | Purpose | Categories of Individuals | Lawful Basis for Processing | Categories of Personal Data | Recipients | Third Countries (outside EEA) |
| 1. | Healthcare provision including diagnosis, care and treatment | Provision of high quality, safe effective and personalised care | * Current patients * Prospective patients * Former patients * Carers/parents | Legitimate interest | * Name * Address/contact details * Date of birth * NHS number * Dental Plan registration * Health condition * Diagnoses * Care and treatment * Special tests | * Data Subjects, their authorised carers, advisors and trustees * Referral practices * Hospitals * Laboratories * Software companies (patient data) * Dental Plan company * Insurers * NHSBSA | *n/a* |
| 2. | Employment of staff | Lawful employment, taxation, pensions administration  Performance management  Skills maintenance and enhancement  Disciplinary and grievance procedures | * Staff members * Prospective staff members * Former staff members | Fulfilment of contract  Legal Duty | * Name * Address/contact details * Date of birth * Health condition (e.g. medical certificates) * National Insurance number | * Data Subjects * Department of Work and Pensions * HM Revenue and Customs * Healthcare Regulators * Software companies (payroll systems) | *n/a* |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Business Function | | Purpose | Categories of Individuals | Lawful Basis for Processing | Categories of Personal Data | Recipients | Third Countries (outside EEA) |
| 3. | Clinical care (by contracted third parties) | Contractual fulfilment  Provision of high quality, safe, effective and personalised care | * Self-employed associate dentists * Self-employed dental care professionals | Fulfilment of Contract | * Name * Address/contact details * Date of birth * Health condition | * Data Subjects * Authorised advisers (e.g. solicitors, accountants) * NHSBSA | *n/a* |
| 4. | Business management - advisory | Contractual fulfilment  Lawful, effective and sustainable business management | * Maintenance contractors * Accountants (individuals) * Solicitors (individuals) | Fulfilment of Contract | * Name * Address/contact details | * Data Subjects * Past/prospective owners of the business * HM Customs and Revenue | *n/a* |
| 5. | Marketing *[if applicable]* | Business promotion, advertising | *[As appropriate]* | *[Consent: opt-in]* | *[If appropriate]* | *[If appropriate]* | *[If appropriate]* |
| 6 | *[Any other purpose e.g. additional services offered]* |  |  |  |  |  |  |

*(Delete or insert rows and categories as appropriate)*

Audit completed by *(Name)* …………………………………………………

Position ………………………………………………….

Date: ………………………………………………….

Review Date: …………………………………………………

**Guidance on Retention of Records in Dental Practice**

*Explanatory Notes*

The Data Protection Bill, incorporating the EU General Data Protection Regulation (GDPR) which will become UK law from 25th May 2018, requires all Data Controllers to “document all the processing of personal data” which they carry out, including the period for which data are retained.

**What the law requires**

* Article 30 of the GDPR sets out explicitly what ‘documentation’ is required, and this includes (Art.30(f)): “…where possible, the envisaged time limits for erasure of the different categories of data”
* The Information Commissioner’s Office (ICO) suggests that these time limits may be set “by internal policy or industry guidelines”.
* Article 5 of the GDPR sets out the six data protection principles, the fifth of which says that data: “Shall be kept in a form which allows identification of data subjects for no longer than is necessary…” but goes on to say that secure archiving is allowed subject to safeguards and “in the public interest or for scientific, historical or research purposes”
* Articles 17 and 19 cover the data subject’s “right to erasure” of their data and provides two relevant circumstances in which this right is over-ridden: performance of a “public duty” or “for the exercise or defence of legal claims”
* Within the General Dental Services (NHS) there is a mandatory requirement to keep patient records for a minimum of two years

None of the above specifies *maximum* periods for data retention. The following are examples of “industry guidance”:

* The Information Governance Alliance ‘Code of Practice for Records Management in Health and Social Care 2016’ (RMCoP) sets out the recommended NHS guidance (see table below)
* Dental indemnity bodies have referred to the above and suggest a maximum retention period of 30 years, and…
* The British Dental Association (source noted in NHS Records Management 2009) has regard to relevant statute such as the Consumer Protection Act 1987 and has recommended 11 years retention for adults and for children when they attain 25 years of age or 11 years whichever is the longer (all measured from the date of the last record entered)
* It is recognised that some electronic records, i.e. those held on proprietary practice management software may not be erasable, however, software suppliers must ensure security of archived data and it must be supplied to the data controller on expiry of contract

**The RMCoP**

Here are some relevant extracts from the IGA/NHS recommendations which may assist for patient clinical data. Other data categories are listed in the attached template:

|  |  |  |  |
| --- | --- | --- | --- |
| Data Category | Start of  Retention Period | Recommended Minimum Length  of Retention | Comment |
| NHS GDS patient notes not included below | Date of last entry | * 15 years | As recommended by NHS |
| Patients undergoing treatment for cancer | Date of diagnosis | * 30 years or 8 years post mortem |  |
| Patients with long term or recurrent disease | Date of last entry | * 20 years from discharge or 10 years after death | Could include chronic unresponsive periodontal disease |
| Clinical Audit | Date of creation | * 5 years | Where personal data is identifiable |
| Patients where serious incidents occurred | Date of incident investigation closure | * 20 years |  |
| Patients where minor incidents occurred | Date of incident investigation closure | * 10 years |  |
| Patients involved in complaints or litigation | Date of resolution or completion of litigation | * 10 years after closure |  |

* See: <https://digital.nhs.uk/information-governance-alliance/>
* <https://www.nhsx.nhs.uk/information-governance/guidance/records-management-code/records-management-code-of-practice-2021/>

**The Template**

In the absence of any specific and clear authoritative guidance, it is for each Data Controller to set the “reasonable period” for retention of each category of data and to be prepared to justify this as “necessary”.

The attached template suggests how dental practices *may* choose to set out their compliance with this requirement. Although times are given, these must be assessed and varied according to individual circumstances and taking into account the rights of the data subject and the general guidance (which may be subject to revision in the future) given in these Notes.

There is no need to advise the ICO or other regulator in advance of these details, but the information must be supplied on request.

*These notes and any comments shown in square brackets […] should be deleted before saving the template below as a Retention Schedule.*

**Data Retention Schedule**

Under the Data Protection Act 2018 and the General Data Protection Regulation

Oak House Dental Practice

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Data Category | Commencement of Retention Period | Minimum Recommended Retention Period | Maximum Duration of Archived Retention | Notes |
| Patient clinical data – adults (unless listed below) | Discharge or last entry in record | * 11 years | * 30 years | Maximum retention period as advised in IGA RMCoP 2016\* |
| Patient clinical data – children (unless listed below) | Discharge or last entry in record | At age 25 (or age 26 if last entry at age 17) or 11 years whichever is the later | * 30 years | As above & British Medical Association recommendation for General Practice records |
| Patient clinical data for those with long-term unresponsive clinical conditions | Date of last entry in record | *[Insert if desired]* | * 30 years | IGA RMCoP |
| Clinical audit records | Date of audit |  | * 5 years | Where identification of individual patients is possible (IGA RMCoP |
| Staff records, Occupational Health records | Date of leaving |  | * 6 years | IGA RMCoP |
| Staff records: radiological dosimetry results | Date of record |  | * 40 years | IRR legislation 1999 |
| Staff records: timesheets | Date of creation |  | * 2 years | IGA RMCoP |
| Contracts for services | Date of cessation of contract |  | * 6 years | e.g. self-employed staff or maintenance contracts (Statute of Limitations) |
| Financial records | Date of completion of record |  | * 6 years | HMRC recommendation: look-back period |
| Telephony recordings | Date of recording |  | *[insert according to circumstance]* | Many recordings will be transcribed and over-written in a short period – possibly one week, but in the event of a serious issue should be retained for disclosure |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Data Category | Commencement of Retention Period | Minimum Recommended Retention Period | Maximum Duration of Archived Retention | Notes |
| Subject Access Requests | Date of supply of information |  | * 3 years | IGA RMCoP |
| CCTV records | Date of recording |  | * 3 months *[or insert]* | Duration of time necessary e.g. to report and investigate crime |
| Software licences | Date of inception |  | * Lifetime of software | Data must be supplied to data controller and erased when contract expires |
| Significant incident log | Date of incident |  | * Major – 20 years * Minor – 10 years | IGA RMCoP  Non-clinical – 12 years advised |

\*Medical Records Code of Practice (2016): Information Governance Alliance/DHSC/NHS Digital

|  |  |  |
| --- | --- | --- |
| Signature of Data Protection Officer/Data Controller: *[delete as appropriate]* |  | Andy Ridout |
| Print Name: |  | Andrew Ridout |
| Review Date: |  | 12th February 2022 |

**Cookies Policy**

*Explanatory Notes*

If you have a practice website, you will almost certainly need to update your Cookies Policy on or after 25th May 2018 when GDPR comes into force in the UK.

Your website designer or software design platform may already have contacted you about this. The important fact is that GDPR significantly expands the notion of a “Data Subject”.

Under the Data Protection Act 1998, data privacy was related to the identification of “living persons”. Under GDPR (Article 4 and Recital 30), this now extends to any “identifier” which “directly or indirectly” could identify a Data Subject.

This may include such things as IP addresses (Internet Protocol address) or URLs, which are basically the internet addresses of your computer, laptop or network. Cookies may collect this data to do their work. There is still some dispute amongst experts as to the extent to which this activity actually breaches an individual’s privacy, but the current consensus is that it does.

The “lawful basis” for carrying out such processes may be “Consent” or “the Legitimate Interests” of the Data Controller. Given that persons browsing your practice website may be complete strangers, “Consent” is the more likely option. Under GDPR, this must be “specific, explicit and freely given”. So your website needs to have a pop-up banner identifying the fact that it has Cookies on it and giving the user the option to click on “Consent” or “Find out more”. The “Find out more” tab should lead to your Cookie Policy and to separate options to block categories of Cookie (see Template). Under GDPR, neither the summary banner nor the consent options should contain pre-ticked boxes.

Each website will have its own individual usage of Cookies and in the Template below we summarise the common types. Some are more inquisitive than others, for instance they may request and store the log-in details of an enquirer and/or enable the site to “remember” that user and their preferences (e.g. type size or language) the next time they log in. it depends on how complex or interactive your site is.

Please therefore remember that the template Cookie Policy on the next page is indicative only. It may include Cookies you do not use, or exclude ones that you do: it is simply a guide. You should check with your web designer or website software supplier to check which applies to you and which Cookies are actually present.

Finally, under GDPR it should be as easy for a Data Subject to withdraw consent as to give it. Your Privacy or Cookies Policy should be easily accessible and enable a user to modify their consent using tick-boxes.

(You should also be aware that Cookies are expressly covered by PECR- the Privacy and Electronic Communications Regulations 2011, which are coincindentally, also being revised. (These Regulations prohibit the staorage of any information on a user’s equipment unless the user is fully informed of the storage and has given consent.)

**Cookie Policy Template**

Oak House Dental Practice

**What are Cookies?**

Your Privacy online is important to us. As is usual with the majority of websites, this site uses Cookies, which are small text files that are automatically downloaded to your computer in order to improve your browsing experience. In this Policy, we describe what information they collect, how we use it and why we sometimes need to store these Cookies. We will also share with you how to prevent Cookies of different kinds being stored, but please note that doing this may interfere with this website and its operation.

* For more information on Cookies, go to: [www.AboutCookies.org](http://www.AboutCookies.org)

**How we use Cookies**

We use Cookies for a number of reasons which are set out in the sections below. Unfortunately, there are no standard options for disabling all Cookies completely without damaging the features they add to a website. You can choose your options at the end of this Policy.

**Disabling Cookies**

You can prevent the setting of Cookies by going to your web browser settings (go to the Help page in the browser menu). Depending on your browser type, you may be able to choose which types of Cookies you disable.

**The Cookies we set**

There are different types of Cookie. We use the definitions of the International Chamber of Commerce.

* (See: <https://www.cookielaw.org/media/1096/icc_uk_cookiesguide_revnov.pdf>)

1. **Strictly Necessary Cookies**

These Cookies are essential for you to be able to move around our website and use its features. They do not collect information that can be used to contact you outside this site, and they do not remain on your device after you have finished looking at this site (known as “session Cookies”).

1. **Performance Cookies**

These Cookies collect information about how visitors use our website, such as which pages are viewed, how often, and whether it is working well. This data is used only when aggregated and does not identify you as a single visitor. These Cookies may be sent to a third party, such as Google analytics so that we can see how many people (but not who they are) have used our site. These are also session Cookies.

1. **Functionality Cookies**

These Cookies allow our website to remember any preferences you have such as text size. They may also allow you to watch videos, blogs or access our social media pages, or to leave comments or messages for us. These Cookies may remain in place for a time after you have left our website (“Persistent” Cookies).

1. **Targeting Cookies**

These Cookies are used by third parties to deliver advertisements which are more relevant to you and measure how effective advertising campaigns are. These Cookies will also persist after you leave our website.

**Choosing your Preference**

Please tick the boxes for which you are happy for us to continue using Cookies:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| |  |  |  |  | | --- | --- | --- | --- | | 1. Necessary | 1. Performance | 1. Functional | 1. Targeting |   *[Delete if not required]* |

You can return to this page and change your preferences at any future visit.

**Information Security**

*Notes*

The Data Protection Act 2018 and the General Data Protection Regulation (EU) require that appropriate technical and other measures are taken to secure and protect all personal data, including patient data, from loss, destruction, corruption and unauthorised/unwarranted access or disclosure.

In addition, the General Dental Council *Standards for the Dental Team* requires that:

|  |
| --- |
| 4.2 You must protect the confidentiality of patients’ information and only use it for the purpose for which it was given  4.3 You must only release a patient’s information without their permission in exceptional circumstances  4.5 Keep patients’ information secure at all times, whether your records are held on paper or electronically |

Failure to adhere to the practice’s Information Security policy therefore may incur serious criminal, financial and professional penalties and loss of reputation.

Dental practices may ‘process’ (that is, obtain, hold, update, store, disclose and destroy) personal data in a wide variety of ways and formats, from the (now rare) instance of paper-only record-keeping to fully digital, “paper-free” networks where the master data may be held remotely and possibly overseas.

Equally, dental personnel may be unacquainted with the technology of digital data storage, or may be highly skilled in the digital environment.

As such it is impossible to adequately describe, deploy or implement a ‘standardised’ Information Security Policy and only a broad indication can be provided.

It is recommended that a wide view is taken of existing resources available online including:

* <https://digital.nhs.uk/information-governance-alliance>
* <https://ico.org.uk/for-organisations/sme-web-hub/checklists/assessment-for-small-business-owners-and-sole-traders/>
* <https://www.sans.org/uk/>

A summary Policy template follows, however, this must be configured and where necessary expanded or edited to suit the circumstances of your practice.

It is also essential that all staff, including contractors who have access to personal data or systems agree to comply with the practice’s information Security policy and understand that a failure to comply may result in disciplinary action and potentially to termination of their employment/engagement in serious or repeated instances.

Regular training and updates should be undertaken for all relevant staff, and audits carried out where practicable to ensure that vigilance is maintained.

**Information Security Policy**

Oak House Dental Practice

1. **General**

The Oak HouseDental Practice takes seriously its obligations, both in law and against professional standards, to maintain a high standard of security around all data which it holds and processes, and particularly personal and special (health) data (as defined in the Data Protection Act 2018 and the General Data Protection Regulation (EU)).

|  |
| --- |
| * Name Andrew Ridout Contact Details [denplandentist@btconnect.com](mailto:denplandentist@btconnect.com)   is designated as the Information Security Officer for the practice and;   * Name: Andrew Ridout Company: Oak House Dental Practice   Contact Details [denplandentist@btconnect.com](mailto:denplandentist@btconnect.com) is designated as the Technical Support Advisor |

All issues related to Information Security shall be reported to the information Security Officer without delay.

1. **Access to Personal Data – Digital**

All employees and contractors with access to personal data held by the practice must adhere to the following requirements:

1. A personal log-in and secure password (as approved by the practice) must be used on each occasion that digital data is accessed
2. Under no circumstances shall the password be divulged to any other person nor shall it be written down or stored on any device
3. Passwords must be changed annually.
4. No personal data shall be accessed or processed in any way other than for the purposes it was obtained as set out in the practice’s Privacy Statement
5. All computers and other devices must be locked to a secure screen-saver mode when not in active use
6. Computers and other devices shall not be used so as to permit any unauthorised viewing or processing of personal data
7. No personal data shall be copied, downloaded or transmitted to any device or storage medium other than those authorised by the Information Security Officer
8. No applications, programs or other functionality shall be downloaded or placed on any practice computer or device other than those authorised by the Information Security Officer
9. Extreme care shall be taken when opening any file attachment originating outside the practice and in any case of doubt the Information Security Officer shall be advised before so doing
10. No information about practice systems, log-in or other technical details may be provided to any person without the authority of the Information Security Officer
11. No device or computer may be connected to the practice internet router or any server without the prior consent of the Information Security Officer
12. **Environmental Security**

All employees and contractors of the practice must adhere to the following requirements to ensure that the practice maintains security around personal data:

1. All patient records, radiographs, correspondence and other items which can identify an individual person shall be kept in a secure location which is locked or suitably protected from unauthorised access as approved by the Information Security Officer
2. The practice premises must be securely locked against unauthorised entry when closed and any alarms must be set and checked by those authorised to do so
3. All desks and work surfaces shall be cleared of material which could identify an individual person when not in use including telephone and other notes
4. Incoming telephone recording messages shall be cleared and deleted from the system once they have been actioned
5. No material which can identify an individual person shall be left in such a position that it can be viewed by unauthorised people
6. CCTV recordings which may depict individual persons shall be deleted from the system at 7-day  intervals
7. **Internet and External Security**

The practice will apply suitable security programs to all systems so as to prevent the introduction of malware or allow unauthorised access, including but not limited to firewalls and anti-virus software as approved by the Information Security Officer and/or the Technical Support Adviser. All software, including the above, will be regularly updated as required.

Penetration testing of the computer, security and telephone systems may take place

at intervals and may not be advised in advance to staff and contractors who should therefore maintain vigilance at all times

1. **Data Back-up**

All personal data will be backed-up on a daily basis using personnel, processes and devices as approved by the Information Security Officer. Back-ups will be audited and confirmed as effective on a regular basis.

1. **Off-site Data and Security**

Where the information Security Officer has authorised that any personal or other data may be taken or transferred off-site (outside the practice location):

1. All such authorisations shall be written and a record kept
2. Authorised data and devices shall be used only for the purposes and period authorised
3. The requirements in Clause 2 of this Policy will apply to all such instances
4. Any loss or damage to devices or data must be *immediately* reported to the Information Security Officer and a Data Breach notification template prepared
5. Devices and data must be secured and out of sight to unauthorised persons whilst in transit and shall be kept in a locked environment when not in use
6. **Financial Data**

When digital payments are taken from patients or other parties at the practice, all staff or contractors will:

1. Ensure that the requirements of the EFTPOS (Electronic Funds Transfer – Point of Sale) device/s and systems supplier are followed at all times
2. Ensure that PCI (Payment Card Industry) best practice guidance is followed
3. Take all precautions against fraud or misuse of payment cards
4. In particular ensure that no payment card details are written down
5. **Internet and E-mail Use**

All staff and contractors will follow the practice rules for use of the internet and e-mails and adhere in particular to any requirements or restrictions on:

1. Personal internet browsing
2. Sending or receiving personal e-mails
3. The encryption of authorised practice e-mails containing patient or other personal data
4. **Destruction of Data**

Data shall only be destroyed with the explicit written consent of the Information Security Officer and using methodology which is secure and approved. Paper data such as notes, jotters which contain personal information will be shredded on the premises or using an authorised contractor.

Devices to be de-commissioned will have all data securely removed from them using an authorised contractor: it is acknowledged that routine formatting or factory re-setting will not suffice.

1. **Other**

All staff and contractors shall at all times take utmost care and diligence in protecting all data, including personal and health-related data, within the practice.

The practice undertakes to regularly train and update staff on the processing of data held, whether digital or otherwise in order to assure the competence of all users and maintain awareness of data protection and information security.

All and any concerns about the security of data held by the practice, however apparently slight, shall be brought at once to the attention of the Information Security Officer and it shall be the policy of the practice that any such information shall be positively and constructively received to encourage prompt and vigilant awareness of the importance of data security.

Any breach of the terms of this policy may lead to disciplinary action against staff or contractors and repeated or serious breaches may be regarded as serious misconduct resulting in termination of employment or engagement.

**Data Protection Policy Statement**

**General**

We shall collect, hold and process personal data in accordance with the provisions of the Data Protection Act 1998. These provisions apply to personal data held on an employee’s personal file or on any associated or computerised record.

**Key Principles**

Where data is held under the provisions of the Data Protection Act 1998, we will ensure that personal data is:

* Fairly and lawfully processed
* Processed for specified purposes
* Adequate, relevant and not excessive
* Accurate
* Not kept for longer than is necessary
* Processed in accordance with individuals rights
* Secure
* Not transferred to countries without adequate protection

**Your Rights**

* Where consent is required, we will obtain your consent before processing data that relates to you
* You are entitled, upon request, to be informed whether personal data about you is being processed, and to be provided with a description of the data, any information available as to its source (if known), the purposes for which it is being processed, and details of the recipients to whom it is being disclosed. We will provide this information upon request although we reserve the right to make a charge for providing this information. In certain circumstances and upon request, we will stop processing personal data about you if it is likely to cause substantial damage or distress to you or someone else. Any requests relating to the above should be made in writing to our Data Protection Officer, Andrew Ridout
* We will endeavour not to make any decisions that significantly affect you which are based solely on automatic processing of personal data. However, where such a decision is made, you will be informed of the way in which the decision was made and be given an opportunity to make representations to challenge the decision. In such circumstances, we will consider your representations and review the decision with a view to ensuring that a correct and fair decision is made

**Your Obligations**

* You are required to make yourself familiar with and follow our Data Protection Policy and Code of Practice, which sets out the way in which we require personal data to be treated in order to comply with the law.
* Personal data is confidential and is held solely for the purpose of carrying out company business. Breach of our Data Protection Policy or Code of Practice may amount to misconduct and result in disciplinary action. Persistent breaches or a serious breach may result in your dismissal.

**Security**

We will ensure that appropriate measures are adopted to guard against unauthorised and unlawful processing, or the accidental loss, destruction of or damage to data.

**Assistance**

The subject of data protection is a complicated one. If you require guidance or assistance you should contact our Data Protection Officer who will be pleased to help you and answer any queries that you may have.

**Social Media**

This applies to all employees who create or contribute to social media, including but not limited to social networks, blogs, wikis and online forums.

It is important to remember what you do online is ultimately linked to your personal life, your professional reputation, and the reputation of Oak House Dental Practice.

Below are **Oak House Dental Practice** guidelines for personal and business use of social media.

**Personal Use**

* Oak House Dental Practicerespects an employee’s right to participate in social media for personal reasons during non-work hours
* All employees are expected to be professional when participating in social media and online commentary
* Any content posted on online forums, should comply with our practice’s confidentiality protocols, Data Protection Acts and GDC guidelines. Do not refer or discuss patients on any online forum, even if a patient is not mentioned by name, they may still be identified through the nature of the discussion
* Any work-related comments should be meaningful, respectful and relevant in a way that protects the practice’s image and reputation and reflects positively on colleagues
* Your actions captured via images, posts or comments may be considered by some as a reflection on our practice, regardless of whether or not it occurs during work hours
* Ask your colleagues permission to post any images of them taken on social events
* To avoid any potential conflicts of interest, employees of Oak House Dental Practiceare not to accept any patients as ‘friends’ or ‘followers’ on their social networking sites. Employees are to direct and encourage patients to join the practice’s social networking sites instead

**Business Use**

We will monitor our social media sites regularly to ensure that we engage with our audience and to monitor content.

Contributions must:

* Be accurate (where they state facts)
* Be genuinely held (where they state opinions)
* Comply with applicable law in the United Kingdom and any country from which it is posted
* Conform to the GDC’s guidance at:
* <https://www.gdc-uk.org/docs/default-source/guidance-documents/guidance-on-using-social-media.pdf?sfvrsn=de158345_2>
* <https://www.gdc-uk.org/docs/default-source/guidance-documents/guidance-on-advertising.pdf>
* Comply with the Advertising Standards Authority; they must be legal, decent, honest and truthful.
* Reflect a caring and competent approach.
* Comply with the terms, conditions and policies belonging to specific social networks and respect copyright laws and reference or cite sources appropriately.
* Comply with our practice’s confidentiality protocols, Data Protection Acts and GDC

Contributions must **not** be:

* Regarded as misleading or unsubstantiated
* Be defamatory, unlawful, obscene, offensive, hateful, abusive or inflammatory
* Discriminate for any reason, such as race, sex or religion; be likely to harass, upset, embarrass, or alarm any other person
* Contain an instruction, advice, or content that could cause harm or injury to individuals or to computers or systems
* Give the impression that the contribution has been posted by Oak House Dental Practiceif this is not the case
* Encourage anyone to commit any unlawful or criminal act or condone any unlawful or criminal act
* Contain any advertising

We reserve the right to remove or to disable access to any contribution which we deem to be in breach of our content standards.

In addition…

* Always gain consent from patients before posting their testimonial, photograph, video or mentioning them on our social network sites
* If a patient posts negative feedback regarding our practice this needs to be dealt with quickly showing a caring and responsible approach. NotifyAndrew Ridoutimmediately
* If a patient posts a complaint follow our complaint handling procedures, notifying Andrew Ridoutimmediately
* If you disagree with another’s opinion or the situation is becoming antagonistic or controversial (for example political, religious debates), politely disengage from the dialogue and talk with Andrew Ridoutimmediately

**Breaches**

When we consider that a breach of our social media policy has occurred, we may take any action we deem appropriate including disciplinary proceedings.