Data Protection, Confidentiality and Information Security Policy

Policy Statement

Vitaliteeth Dental Spa processes personal data that relate to employees and patients and is therefore required by law to comply with the data protection regime, which protects the privacy of individual personal data and ensures that they are processed fairly, lawfully and proportionately.

The (UK) General Data Protection Regulations (UK GDPR), the Data Protection Act (2018) and the Data (Use and Access) Act 2025 are the data protection regime for the UK. The DPA 2018 is the UK implementation of the GDPR.

The Practice is committed to ensuring that it complies with the GDPR and applies ethical principles to all aspects of its work to protect the interests of employees and patients and maintain the confidentiality and security of any personal data held in any form by the practice. To do this, Vitaliteeth Dental Spa will comply with the data protection principles. In summary, these state that personal data shall be:

- fairly and lawfully processed in a transparent manner
- processed for limited purposes (i.e. obtained only for specified and lawful purposes and further processed only in a compatible manner)
- adequate, relevant and not excessive (data minimisation)
- accurate and up to date
- not kept for longer than is necessary (storage limitation)
- processed with integrity and confidentiality (security)
- accountability e.g. demonstrates compliance with above principles

We also recognise the rights of individuals under UK GDPR:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure

- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision-making including profiling

The Practice has developed a UK GDPR Privacy Notice for Patients and a UK GDPR Privacy Notice for Staff. These notices are kept up to date, amendments are tracked. The notices are available from the Data Protection Lead.

Lawful Basis

Our lawful bases for processing personal data are:

Patients

Our lawful bases for processing patient personal data are:

- Legal Obligation – to comply with UK law, NHS Scotland requirements, clinical record-keeping duties, and professional standards.
- Public Task – for the provision and management of NHS dental services as part of NHS Scotland's healthcare system.
- Contract – to provide private dental treatment, manage appointments, and process payments.
- Legitimate Interests – for limited administrative purposes such as security (e.g., CCTV), where this does not override your rights.
- For special category health data, we rely on Article 9(2)(h) – processing necessary for the provision of health care and treatment.

Staff

Our lawful bases for processing staff personal data are:

- Contract – to enter into and manage employment or contractor agreements, including payroll, rotas, training, and performance management.
- Legal Obligation – to meet employment law, HMRC requirements, health & safety duties, PVG checks, and regulatory obligations such as verifying GDC registration. Legitimate Interests – for practice management purposes such as security (e.g., CCTV), IT monitoring, and ensuring service quality, where this does not override staff rights.
- Public Task – for staff involved in delivering NHS-funded dental services as part of NHS Scotland's healthcare system.

- For special category data, such as health information or occupational health records, we rely on: Article 9(2)(b) – processing necessary for employment law obligations. Article 9(2)(h) – processing necessary for occupational health and the management of healthcare services.

Responsibilities

This Data Protection, Confidentiality and Information Security Policy applies to all practice employees and any others who have legitimate rights to access and use the practice's information systems.
Compliance with the UK GDPR and this policy is the responsibility of all practice employees and everyone who has access to practice records. A breach of this policy, whether deliberate or through negligence, could lead to disciplinary action being taken and possible investigation by the General Dental Council. A breach of the UK GDPR could also lead to criminal prosecution.
The following table lists key responsibilities among the dental team

Dental Team Member	**Responsibility**
Vitaliteeth Limited	Data Protection, Confidentiality and Information Security policy; deals with subject access requests made under the UK GDPR and requests made under the Freedom of Information Act (Scotland) 2002; training of staff regarding data protection and confidentiality.
Daniela Zara (Senior Audit Officer and in-house Data Protection lead)	Data Protection, Confidentiality and Information Security policy; deals with subject access requests made under the UK GDPR and requests made under the Freedom of Information Act (Scotland) 2002; training of staff regarding data protection and confidentiality.
Mr Nikolaos Vourakis	Data controller (Associate Dentist who 'owns' a patient list)
Dr Yehyah Hamandi	Data controller (Associate Dentist who 'owns' a patient list)

Mohamed Magdi Mohamed Helmi Banoub	Data controller (Associate Dentist who 'owns' a patient list)
All staff	Compliance with the UK GDPR and this Data Protection, Confidentiality and Information Security policy

*The Data Protection Officer is a requirement under the DPA 2018. Duties of the DPO cover all personal data processing activities. Specific responsibilities include:

- informing, advising and monitoring compliance of the staff with data protection obligations
- monitoring compliance of the practice's data protection polices in line with the UK GDPR, including managing internal data protection activities, raising awareness of data protection issues, training staff and conducting internal audits
- advising on data protection impact assessments where these are required
- cooperating with the (UK) Information Commissioners Office (ICO)
- being the contact for the (UK) ICO and for individuals whose data is processed (employees, patients etc).

If you have any questions or comments about processing personal data or this policy, please contact the dataprotection@vitaliteeth.co,uk

Definition of Personal Data Covered Under the UK GDPR

The UK GDPR applies to personal data, which is defined as information which relates to a living individual who can be identified from the information itself or by linking it with other information. This includes an individual's name, address or email address, an online profile or an employee's HR record, sickness absence or appraisal record. There is also 'special category' information which relates to sensitive personal data such as medical information, ethnic origin etc. The UK GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria.

To provide effective care for patients and provide care within the NHS system, the Practice processes personal data of patients. Personal data means practically any information about, or correspondence relating to, a named individual. It includes both facts (e.g. treatment a patient has had) and opinions (e.g. any concerns the patient or dental team might have about the patient's dental health), including:

- personal information and contact details, including the patient's name, address and date of birth
- dental, social and medical histories (e.g. past or current medical conditions, current medication, the name of the patient's GP, special needs)
- results of the examination of the patient's mouth and oral health, including radiographs and clinical photographs
- information about appointments
- any treatments and the costs
- any proposed care, including advice given to the patient and referrals the patient might need
- any concerns that the patient or dental team might have
- details of the patient's consent for specific procedures
- correspondence with other healthcare workers that relates to the patient's care.

As an employer, the Practice also processes the personal data of employees, including:

- personal information and contact details, including name, address and date of birth.
- health clearance and immunisation status
- employment and educational histories
- leave records
- performance and appraisal information
- information on training and professional development

Procedures for Ensuring Compliance with the UK GDPR and the Confidentiality and Security of Personal Data

All Staff

To maintain a good patient–dental team relationship, it is essential that patients feel they can provide personal information to dental team members with the knowledge that this information will be kept securely and not shared unlawfully. It is also important that patients are able to provide, in confidence, full details of their medical, social and dental histories to facilitate safe and effective care. To achieve this, all staff must follow the procedures listed below.

- Comply with the data protection principles and the General Dental Council principles set out in the 'Standards for the Dental Team'
- Undergo training in processing personal data, confidentiality and information security.
- Keep any personal data or confidential data that they hold, whether in electronic or paper format, securely, which includes:
  - storing paper files with personal data in lockable filing cabinets that are locked when authorised staff are not present to monitor access
  - storing electronic files containing personal data on password-protected computer systems
  - 'screen-locking' unattended computers
  - not sharing computer passwords with unauthorised people, not writing down passwords and not keeping passwords on or near their computer
  - not forwarding emails containing personal data to internet email accounts as these are not secure
  - holding personal data on laptops only where there is a clear business necessity and permission is sought from the Practice Manager (if there is a necessity, ensure it is fully encrypted)
  - avoiding carrying personal data on removable media (e.g. memory sticks)
  - not using unlicensed software on Practice computers
  - ensuring windows and doors are secured if you are the last to leave the practice
- Practice good record-keeping, and ensure records are:
  - accurate
  - dated
  - contemporaneous
  - comprehensive
  - secure
  - legible and written in language that can be read and understood by others, and is not derogatory
- Maintain the confidentiality of any personal data by, for example:
  - ensuring that personal information is not disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third party (e.g. avoid working on

personal data such as application forms on public transport, do not discuss identifiable information about patients with anyone outside the practice, including friends, family and schools, or leave messages about a patient's care with an unauthorised third party or on an answering machine) (NB: this also applies after termination of employment)

- respecting patient privacy for discussions of a sensitive nature (e.g. discussion of medical information, payment, or asking patients for proof of exemption status)
- using personal data only for the purposes for which they are authorised in the relevant Data Protection registration.

- Ensure patients know what information is to be shared, why it is being shared and the likely consequences of sharing (or not sharing) the information and give patients the opportunity to withhold permission to share their information.
- Share personal data only on a 'need to know' basis and following consent from the patient, for example:
  - to another health professional for the provision of effective care and/or treatment
  - to ensure the provision of care under the NHS (e.g. payment claims, information for health boards)
- Check that any personal information that you provide in connection with your employment is accurate and up to date, and inform the Practice Manager of any changes to this information
- Inform the Data Protection Officer or the Data Protection Lead, who are responsible for ensuring compliance with the UK GDPR and this policy, of any suspected or actual breach of the UK GDPR or this policy.

Data Controllers

Data controllers are those who hold personal records (e.g. dentists who are the 'owner' of their own patient list). All data controllers must follow the procedures detailed above for staff, and the procedures listed below.

- Register with the UK Information Commissioner's Office
- Keep the details of the registration up to date
- Renew this registration annually

General Practices

- All staff contracts and agreements include a clause regarding confidentiality of personal data
- Keys for lockable storage cabinets are held only by dental team members who require regular access to the information they contain. Keys are stored in a safe place/secure key cabinet
- Practice computers have a full audit trail facility to prevent deletion or overwriting of data
- Each computer is fitted with anti-virus software
- Daily back-ups of the Practice's electronic records are made, and held in a fireproof safe
- Weekly back-ups of the Practice's electronic records are made and held off-site
- Back-ups are tested to ensure data can be retrieved in a useable format
- Adult patient records are kept for at least 10 years; child patient records are kept for 10 years. The child record should evolve into the adult record. On death, adult records are kept for 3 years. Where the person dies before their 17th birthday, the record should be held until they would have turned 25.
- Personal data are reviewed, updated and deleted in a confidential and secure manner when no longer required
- Windows are fitted with locks and the practice is fitted with an intruder alarm that is set each night to increase security
- A continuity plan that includes procedures for protecting and restoring personal data is in place in the event of a major incident

Sharing Personal Information

To provide patients with appropriate care, we might need to share personal data with:

- another dentist or another health professional who is caring for the patient
- the patient's GP
- a laboratory
- NHS payment authorities
- HM Revenue and Customs
- Department for Work and Pensions, if the patient is claiming exemption or remission from NHS charges

- a private dental scheme, if the patient is a member

To fulfil our duties as employers, we might need to share staff personal data with:

- other employers
- HM Revenue and Customs
- pension providers
- educational institutions
- regulatory and professional bodies

In these cases, only the minimum information required will be shared.

Disclosure Without Consent

Exceptional circumstances might override the duty to maintain confidentiality. Where possible, we will inform the patient or staff member of requests to share personal information. The decision to disclose information must only be taken by senior staff. Examples include:

- situations where there is a serious public health risk or risk of harm to other individuals
- when information is required by the police to prevent or detect crime or to apprehend or prosecute offenders (if not providing the information would prejudice these purposes)
- in response to a court order
- to enable a dentist to pursue a legal claim against a patient.

The Data Protection Lead is responsible for making the decision regarding whether personal data should be disclosed. In these cases, only the minimum information required will be shared.

Data Breaches

We will always aim to ensure that the information we hold is held securely. We will report any detected data breaches that are likely to result in a risk to the rights and freedoms of the individuals affected to the ICO within 72 hours of becoming aware of them. We will also

notify the affected individuals if the breach is likely to result in a high risk to their rights and freedoms. We will also inform the ICO of any breach of confidentiality.

We will document all data breaches, even those that are not notifiable to the ICO, and will include information on the steps taken to mitigate any adverse effects and to ensure that the breach does not reoccur.

Data Subject Rights

We recognise the rights of individuals under UK GDPR, and we have processes in place to deal with relevant requests. We provide Privacy Notices (Patients and Staff) to comply with an individual's right to be informed. Where an individual requests access to their information, we will provide this free of charge, and in an electronic and commonly used format within one month of the request, unless we deem the request to be unreasonable or excessive. If we refuse a request for access, we will inform the individual of our decision, and the reasons for it, within one month of their request. We will also inform the individual that they have the right to appeal to the ICO and to seek legal advice.

Where an individual notifies us that the information we hold about them is incorrect, we will rectify this. Where an individual asks us to delete their information, we will consider this based on the type of information and any legal or professional obligations to retain the data. Where we cannot delete the information, we will inform the individual of this within one month of their request. Where an individual asks us to transfer their information to another dental practice, we will ensure that this is done in a confidential and secure manner. Individuals also have the right to object to data processing or to ask for this to be restricted.

We do not use personally identifiable information in automated decision making or data profiling.

Guide to Information last updated: 13/05/2026.

Author: Daniela Zara

Date of next review: May 2027

Document Monitoring

Document Title	Document Version	Issue Date
CP – Company Policy - Data Protection, Confidentiality, and Information Security Policy	V5.0	13/05/2026

Revision History

Reason for Revision	Rev. No.	Approved by	Revision Date
Publication	V1.0	Tracey Hayes	08/03/2023
Review – Addition of Data Controller (Yehyah Hamandi)	V2.0	Daniela Zara	15/11/2023
Review – Addition of Data Controller (Mohammed Banoub)	V3.0	Daniela Zara	27/05/2024
Scheduled review – no changes	V4.0	Daniela Zara	27/05/2025
Scheduled review – change in document format, DPO update, contact update (designated email)	V5.0	Daniela Zara	13/05/2025

The latest approved version of this document supersedes all other versions, upon receipt of the latest approved version all other versions should be destroyed, unless specifically stated that. previous version(s) are to remain extant. If in any doubt, please contact the document's Author.

The following staff have read and understood this policy:

Dental Team Member	Position	Signature	Date