Smile Dental Implants

Data Protection Policy — England & Wales Practice Framework

Regulatory Practice Note: This internal policy establishes a compliance binding agreement between the Practice entity and practice personnel (employees, associates, and non-employed staff). It incorporates requirements under the UK GDPR, Data Protection Act 2018, PECR, and integration frameworks from the Data (Use and Access) Act 2025 (DUAA).

Practice Entity	Smile Dental Implants	**Data Protection Officer**	Dr Dipesh Patel
Applicable Jurisdictions	England and Wales	**Compliance Portals**	dsptoolkit.nhs.uk | DCME Portal

Contents

1. Interpretation & Definitions
2. Introduction
3. Scope of Policy
4. Personal Data Protection Principles
5. Lawfulness, Fairness, Transparency
6. Consent Frameworks
7. Transparency (Notifying Subjects)
8. Purpose Limitation
9. Data Minimisation
10. Accuracy Mandates
11. Storage Limitation
12. Security Integrity & Confidentiality
13. Reporting a Personal Data Breach
14. Transfer Limitation
15. Data Subject's Rights & Requests
16. Accountability Pillar
17. Record Keeping Mandates
18. Training and Governance Audit
19. Privacy by Design & DPIA
20–24. Processing, Marketing, & Caldicott

1. Interpretation

1.1 Definitions:

Automated Decision-Making (ADM): When a decision is made based solely on Automated Processing (including profiling), which produces legal effects or significantly affects an individual.

Automated Processing: Any form of automated processing of Personal Data evaluating personal aspects relating to an individual, specifically analyzing or predicting workplace performance, economic situation, health, personal preferences, or movements.

Caldicott Principles: 8 foundational clinical data principles used across healthcare sectors to ensure people's identifiable information is kept confidential and shared appropriately.

Company Personnel: All practice employees, associate dentists, hygienists, self-employed staff, contractors, agency workers, consultants, and management team members.

Controller: The person or organisation determining the when, why, and how of processing Personal Data. Smile Dental Implants acts as the primary Controller under law.

Data Subject: A living, identified, or identifiable individual about whom we hold Personal Data (including patients, clinical staff, and suppliers).

Data Privacy Impact Assessment (DPIA): Systematic processes used to identify and mitigate operational or clinical data hazards.

Special Categories of Personal Data: Highly sensitive data fields including racial/ethnic origin, political or religious beliefs, physical/mental health details, genetic/biometric files, and sexual orientation profiles. Clinical dental records are managed under these stringent rules.

2. Introduction

2.1 Compliance Mandate: This Policy sets out how we handle the Personal Data of our patients, their parents or carers, employees, and third parties in full compliance with UK GDPR, the Data Protection Act 2018, PECR, and phased elements under the Data (Use and Access) Act 2025 (DUAA).

2.2 Universality: This Data Protection Policy applies to all Personal Data we Process regardless of the system, hardware, interface, or media on which that data is hosted or stored.

2.3 Responsibility: Compliance with this policy is mandatory for all Company Personnel. Failure to adhere to these terms can compromise patient safety and lead to practice disciplinary reviews or professional misconduct escalations.

3. Scope of Policy & Seeking Compliance Advice

3.1 Regulatory Financial Risk: Failure to comply with UK GDPR core frameworks exposes the practice to potential administrative statutory fines of up to £17.5 million or 4% of total worldwide annual turnover, whichever is higher.

3.2 Leadership Accountability: Line managers must actively enforce data governance processes and ensure all personnel complete periodic statutory training tracks.

3.3 Escalation Points: The DPO post is held by **Dr Dipesh Patel**. Personnel must consult the DPO immediately when:

(a) Uncertain about the lawful basis being utilized for a processing activity.

(b) Processing actions rely on capturing complex or Explicit Consent.

(c) A verified or suspected Personal Data Breach has occurred.

(d) Deploying a significant new piece of practice software or change in clinical systems requiring a formal DPIA evaluation.

4. Personal Data Protection Principles

We strictly adhere to core UK GDPR metrics requiring that data is: (a) Processed lawfully, fairly, and transparently; (b) Subject to clear purpose limitation parameters; (c) Restricted via precise data minimisation rules; (d) Verified for accuracy; (e) Governed by tight storage limitation schedules; and (f) Enforced via complete security, integrity, and operational confidentiality controls.

5. Lawfulness, Fairness, and Transparency

5.1 System Controls: Data must only be collected for clear clinical, administrative, or statutory grounds.

5.2 Lawful Gateways: Processing is valid only if at least one basic parameter matches: patient clinical consent, fulfillment of a medical/dental treatment contract, statutory healthcare legal obligations, patient vital interests, or legitimate practice operational interests.

6. Consent Frameworks

6.1 Active Affirmation: Consent requires an unambiguous, active, positive check or signature. Pre-ticked digital boxes or systematic silence do not constitute legal consent.

6.2 Withdrawal Rights: Data subjects hold the right to withdraw clinical or marketing consents at any moment; these entries must be updated inside management systems immediately upon request.

7. Transparency & Notices

We provide comprehensive, clear, and plain-language Privacy Notices to patients at the immediate point of initial data collection. For indirect collection pathways, notices must be evaluated and verified within statutory parameters.

8. Purpose Limitation

Personnel cannot use collected patient information for alternative, incompatible, or detached activities without validating explicit consent tracks or completing formal internal updates via the DPO.

9. Data Minimisation

Only gather, view, or store the specific parameters of data necessary to successfully complete your defined clinical or practice duties. Extraneous or unnecessary profile records must never be logged.

10. Accuracy Mandates

Verify patient demographic and clinical records at regular interactions. Take reasonable operational steps to quickly correct or append erroneous or outdated information fields.

11. Storage Limitation

Data must not be kept indefinitely. Records are kept in accordance with established national dental archive retention pathways. When retention intervals lapse, data must be securely destroyed or permanently anonymized.

12. Security Integrity and Confidentiality

12.1 Technical Measures: Deploy encryption, secure cloud hosting frameworks, and system pseudonymisation wherever appropriate. Exercise strict operational care around Special Category health and clinical record entries.

12.2 Security Pillars: Maintain core data controls across:

(a) *Confidentiality*: Restricting system visibility exclusively to authorized individuals with a verified operational need-to-know.

(b) *Integrity*: Shielding entries against malicious or accidental unauthorized alteration.

(c) *Availability*: Guaranteeing prompt system access to verified operators during critical patient treatments.

13. Reporting a Personal Data Breach

If you discover or suspect an operational data incident, do not attempt an independent check. **Immediately notify the DPO (Dr Dipesh Patel).** The practice will systematically review and triage the issue against ICO rules, ensuring notifications are filed within the critical 72-hour regulatory window when high risks to data subjects are present.

14. Transfer Limitation

Cross-border processing or off-shore server data transfers outside the UK are strictly managed. Transfers require valid UK adequacy regulations, binding corporate rules, or standard contractual safeguard blocks approved for domestic execution.

15. Data Subject's Rights and Requests

Patients hold rights to access (Subject Access Requests), erase, rectify, restrict, or object to specific processing channels. Personnel must verify identity parameters before processing entries and forward all official requests to the DPO within 24 hours of receipt.

16. Accountability Pillar

Smile Dental Implants demonstrates operational compliance through structured tracking tools: maintaining full processing registers, providing verifiable workforce training modules, enforcing data protection protocols by design, and maintaining active clinical feedback loops.

17. Record Keeping

The practice logs clean documentation registers including details on controllers, data type categorizations, processing purposes, downstream processing partners, retention milestones, and existing administrative technical safeguards.

18. Training and Governance Audit

All clinic employees and non-employed healthcare partners must finish core data handling tracks. Core operations, local network frameworks, and software tools undergo systematic governance checks to protect patient rights.

19. Privacy by Design & Data Protection Impact Assessments (DPIA)

The practice implements Privacy by Design measures when processing personal data by choosing appropriate technical and organizational protections (such as Pseudonymisation) effectively to maintain compliance with data privacy principles. You must assess what Privacy by Design safeguards can be added to all software programs, computer networks, or operational processes that handle Personal Data by evaluating the current state of technology, cost factors, and processing risks.

Smile Dental Implants • Quality Governance & Data Protection Framework Document (England & Wales)