

## Data Protection Policy

This policy outlines how the practice complies with the *Data Protection Act 1998* and ensures that personal information is processed fairly and lawfully. The practice only keeps relevant information about employees for the purposes of employment, or about patients to provide them with safe and appropriate dental care.

The Information Commissioner's office is the UK's public body responsible for governance compliance with the DPA and the practice owner is registered as a data controller. All self-employed team members are required to notify the ICO separately and provide the practice of evidence of continued registration. There is a £35 fee, registration is valid for all locations they work at and must be renewed annually.

Team members are expected to be familiar with the eight principles of the Data Protection Act 1998 (which became law from March 2000) and with the practice code for processing and disclosing personal data.

---

### 1. First Principle

"Personal data shall be processed fairly and lawfully

### 2. Second Principle

"Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes".

### 3. Third Principle

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed".

### 4. Fourth Principle

"Personal data shall be accurate and, where necessary, kept up to date".

### 5. Fifth Principle

"Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes".

### 6. Sixth Principle

"Personal data shall be processed in accordance with the rights of data subjects under this Act".

### 7. Seventh Principle

"Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data".

### 8. Eighth Principle

"Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection of the rights and freedoms of data subjects in relation to the processing of personal data

CG Domian 1 Data Security/Data Protection	Author/Owner: E.Harris	Location: Practice Documents ( <a href="#">\\Server K:\ Clinical Governance-Lymington D1</a> )	Review date: 01/11/2018	Version: 2	Page 1 of 3
---	---------------------------	--	----------------------------	---------------	-------------

The Information Commissioners Office has a website with useful guidance around the Act [www.dataprotection.gov.uk](http://www.dataprotection.gov.uk) (general), [www.dpr.gov.uk](http://www.dpr.gov.uk) (notification on-line & the Register)

E-mail [data@dataprotection.gov.uk](mailto:data@dataprotection.gov.uk)

To view the Act please visit the HMSO website [www.legislation.hmso.gov.uk](http://www.legislation.hmso.gov.uk)

### **Processing personal data in accordance with the Data Protection Act 1998**

- The practice processes their personal data provided by patients and team members fairly and lawfully. If required an explanation of how the data is going to be processed can be provided, as well as a copy of this Data Protection Policy.
- Personnel records will only be seen by appropriate management.
- Patients' records will only be seen by appropriate team members.
- All manual and computerised records are kept in a secure place; regularly reviewed, updated and destroyed in a confidential manner when no longer required.
- Patient records will be retained for at least 11 years from when the patient is no longer a patient of the practice, and for children records will be retained at least to age 25, or for 11 years, whichever is longer (Medico-legal organisations suggest that all health records are kept indefinitely).
- Patients have the right to object to personal data being processed as outlined in this policy but it may affect the ability to provide safe and appropriate dental care.

### **Disclosure of personal data in accordance with the Data Protection Act 1998**

- Information the patient consents to share will be disclosed to those who would be unable to provide effective care and treatment without it but will be limited to the minimum required to provide that care (*the need-to-know basis*). This may be a specialist providing care on referral, doctor, hospital, community service, or other health care professional involved in care.
- Personal data may also need to be disclosed on a *need-to-know basis* to NHS authorities, the Inland Revenue, the Benefits Agency (when claiming exemption or remission from NHS charges) or private dental schemes of which the patient is a member.
- The practice will not process any relevant 'sensitive personal data' without prior informed consent. As defined by the Act 'sensitive personal data' is that related to political opinion, racial or ethnic origin, membership of a trade union, the sexual life of the individual, physical or mental health or condition, religious or other beliefs of a similar nature.
- Sickness and accidents records will also be kept confidential.
- In very limited cases, such as for identification purposes, or if required by law or a court order, information may have to be shared with a party not involved in the patient's health care.
- In certain circumstances disclosure is in the public interest and the common law obligation to confidentiality is overridden. e.g. to assist in the prevention or prosecution of serious crime
- In all other cases, disclosure to a third party which is not covered by this policy will not occur without the data subject's express consent.
- Patients and staff have the right to access their records by making a request in writing and paying a fee (up to £10 for computerised records and up to £50 for hard copies). Responsibility for access to health records requests lies with the data controller. A copy of records will be provided within 40 days of the request, with an explanation of the record if required.

CG Domian 1 Data Security/Data Protection	Author/Owner: E.Harris	Location: Practice Documents ( <a href="#">\\Server</a> K:\ Clinical Governance-Lymington D1)	Review date: 01/11/2018	Version: 2	Page 2 of 3
---	---------------------------	--	----------------------------	---------------	-------------

All team members must follow the practice procedures on use of computers, communications, transfer of data, disclosure and handling requests for access to health records.

CG Domian 1 Data Security/Data Protection	Author/Owner: E.Harris	Location: Practice Documents ( <a href="#">\\Server</a> K:\ Clinical Governance-Lymington D1)	Review date: 01/11/2018	Version: 2	Page 3 of 3
---	---------------------------	--	----------------------------	---------------	-------------