Data Protection, Confidentiality and Information Security Policy

Policy Statement

The *Smile Dental Care Dental Practice* processes personal data that relate to employees and patients and is therefore required by law to comply with the Data Protection Act 1998 (DPA), which protects the privacy of individual personal data and ensures that they are processed fairly and lawfully. The Practice is committed to ensuring that it complies with the DPA 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, the *Smile Dental Care* will comply with the eight principles in the DPA. In summary, these state that personal data shall be:

- fairly and lawfully processed;
- 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;
- accurate and up to date;
- not kept for longer than is necessary;
- processed in line with the individual's rights;
- secure;
- not transferred to countries outside the European Economic area without adequate protection.

A shortened 'Data Protection Policy for Patients' has been developed for patients.

Responsibilities

This Data Protection, Confidentiality and Information Security Policy applies to all practice employees and others who have legitimate rights to access and use the practice's information systems.
Compliance with the DPA 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 DPA could also lead to criminal prosecution.
The following table lists key responsibilities among the dental team

Dental Team Member	**Responsibility**
Karen Michie (Practice Manager)	Data Protection, Confidentiality and Information Security policy; deals with subject access requests made under the DPA and requests made under the Freedom of Information Act (Scotland) 2002; training of staff regarding data protection and confidentiality
Eva Constantine	Data controller (i.e. principal dentist who 'owns' a patient list)
Jodie Fulton	Data controller (i.e. associate dentist who 'owns' a patient list)
All staff	Compliance with the DPA and this Data Protection, Confidentiality and Information Security policy

If you have any questions or comments about processing personal data or this policy, please contact the Practice Manager

Definition of Personal Data Covered Under the DPA

The DPA covers all personal data, regardless of the format, that are stored in a 'relevant filing system'. A relevant filing system means any system where information can be found relatively easily, even if it is not by a personalised index or key.In addition, information recorded with the intention that it will be put in a relevant filing system or held on computer is covered.
As an employer and to provide effective care for patients and provide care within the NHS system, the Practice processes personal data of employees and 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 x-rays and clinical photographs;
- information about appointments;
- any treatments and their 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.

Procedures for Ensuring Compliance with the DPA 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 followthe procedures listed below.

- Comply with the 8 principles outlined in the DPA and the General Dental Council principles set out in the '*Standards for Dental Professionals guidance*', and in '*Principles of Patient Confidentiality*' and '*Principles of Patient Consent*'.
- Undergo training in processing personal data and confidentiality.
- 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, ensureit is fully encrypted);
- avoiding carrying personal data on removable media (e.g. memory sticks or CD-roms);
- 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 orally 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 Practice Manager, who is responsible for ensuring compliance with the DPA and this policy, of any suspected or actual breach of the DPA 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.
- Keep the details of the registration up to date and 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 11 years; child patient records are kept for at least 11 years or until the patient is 25 years old, whichever is longer.
- 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 the patient 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;
- the Inland Revenue;
- the Benefits Agency, if the patient is claiming exemption or remission from NHS charges;
- a private dental scheme, if the patient is a member.

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 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.

Eva Constantine is responsible for making the decision regarding whether personal data should be disclosed.

Subject Access Requests

Individuals have a right under the DPA to have a copy of the information held about them on computer and in manual filing systems. This is known as the right of subject access. Parents also have rights to access their children's records if it is in the child's interest. The 'data controller' (i.e. the dentist) must make a judgement if a child or parent requests records (The DPA allows a young person of 12 years or more in Scotland, with sufficient capacity and maturity, to exercise their rights under the Act). A solicitor can request access with the consent of his client.

A data protection policy that outlines the personal data that are processed and the manner in which the data are processed is available for patients.

The Practice Managerdeals with subject access requests and will respond to requests from patients or employees within 40 days of receipt of the request.

The following staff have read and understood this policy.

Dental Team Member	Position	Signature	Date