CONFIDENTIALITY POLICY

Southfield Dental Practice recognises that all members if the team have an ethical and legal duty to keep patient information confidential.

The relationship this practice has with each patient is based on trust that information will not be given to external persons or organisations without the patient's consent.

All members of the practice team are expected to comply with this policy and are advised to be aware of the confidentiality clause within their staff contract. Breaches of this policy could lead to dismissal.

Standards for dental professionals (in the guidance from the GDC) notes that practitioners must 'Protect the confidentiality of patients' information'.

This means:

- Using information only for the purpose for which it is was given
- Preventing information from being accidentally received.
- Preventing unauthorised access by keeping information secure at all times.

Only in exceptional circumstances can breach of confidentiality be justified.

The importance of confidentiality

The relationship between dentist and patient is based on the understanding that any information revealed by the patient to the dentist will not be divulged without the patient's consent. Patients have the right to privacy and it is vital that they give the dentist full information on their state of health to ensure that treatment is carried out safely. The intensely personal nature of health information means that many patients would be reluctant to provide the dentist with information if they were not sure that it would not be passed on. All staff must follow the General Dental Council's rules for maintaining patient confidentiality contained in *Standards for dental professionals* and *Principles of patient confidentiality*. If confidentiality is breached, the dentist/dental hygienist/dental therapist/dental nurse faces investigation by the General Dental Council and possible erasure from the Dentists or DCP Register, and may also face legal action by the patient for damages and, for dentists, prosecution for breach of the 1998 Data Protection Act.

What is personal information?

In a dental context, personal information held by a dentist about a patient includes:

- the patient's name, current and previous addresses, bank account/credit card details, telephone number/email address and other means of personal identification such as physical description
- information that the individual is or has been a patient of the practice or attended, cancelled or failed to attend an appointment on a certain day
- information concerning the patient's physical, mental or oral health or condition
- information about the treatment that is planned, is being or has been provided
- information about family members and personal circumstances supplied by the patient to others
- the amount that was paid for treatment, the amount owing or the fact that the patient is a debtor to the practice.

Principles of confidentiality

This practice has adopted the following three principles of confidentiality:

Personal information about a patient:

- is confidential in respect of that patient and to those providing the patient with health care
- should only be disclosed to those who would be unable to provide effective care and treatment without that information (*the need-to-know concept*), and
- such information should not be disclosed to third parties without the consent of the patient except in certain specific circumstances described in this policy.

Preventing breaches of confidentiality

Keep all confidential data stored securely and do not allow them to be placed in areas where they may be seen by unauthorised personnel. Do not provide information:

- To school about a child's attendance
- To employers about patient's appointments
- To third parties about appointments or leave detailed answer machine messages.
- Only leave messages to return the practice's phone call.

Recall cards and other personal information must be sent in a sealed envelope and marked **'Private & Confidential'**

Disclosure of information

If is necessary to release information about a patient:

- Get patient's consent first, where possible. Make sure they understand what information you will release, why and any likely consequences.
- Release the minimum required.
- Be prepared to justify decisions and follow-on action.

If you are using patient information (i.e. radiographs, study models) for teaching purposes gain the patient's consent and ensure the patient cannot be identified from the information released.

Disclosures to third parties

There are certain restricted circumstances in which a dentist may decide to disclose information to a third party or may be required to disclose by law. *Responsibility for disclosure rests with the patient's dentist and under no circumstances can any other member of staff make a decision to disclose.* A brief summary of the circumstances is given below.

When disclosure is in the public interest

There are certain circumstances where the wider public interest outweighs the rights of the patient to confidentiality. This might include cases where disclosure would prevent a serious future risk to the public or assist in the prevention or prosecution of serious crime.

When disclosure can be made

There are circumstances when personal information can be disclosed:

- where expressly the patient has given consent to the disclosure
- where disclosure is necessary for the purpose of enabling someone else to provide health care to the patient and the patient has consented to this sharing of information
- where disclosure is required by statute or is ordered by a court of law
- where disclosure is necessary for a dentist to pursue a bona-fide legal claim against a patient, when disclosure to a solicitor, court or debt collecting agency may be necessary.

Disclosure of information necessary in order to provide care and for the functioning of the NHS

Information may need to be disclosed to third party organisations to ensure the provision of care. In practical terms this type of disclosure means:

- referral of the patient to another dentist or health care provider such as a hospital.

Data protection code of practice

The Practice's *Data protection code of practice* provides the required procedures to ensure that we comply with the 1998 Data Protection Act. It is a condition of engagement that everyone at the practice complies with the code of practice.

Data Protection Act 1998

The Data Protection Act 1998 (DPA 98) came into force on 1st Mar 2000. The Act sets out procedures to be followed when personal information is processed in both electronic and paper records.

Under DPA 98, most of the Access to Health Records Act 1990 was repealed and now applies only to requests for health records in respect of deceased individuals

The Data Protection Officer (DPO) for Southfield Dental Practice is Christian Gollings.

DPA 98 covers both automated and manual records for living individuals. The Act generally gives them the right of access to all their own health records.

All personal data, written and electronic, must be processed in accordance with the 8 Data Protection Principles. These Principles are set out in this document.

Access to records

Under the Data Protection Act 1998, a patient has the right to see their dental records. This is known as "subject access rights".

This document will guide you in how to respond to subject access requests and it also provides you with guidance with responding to requests from patients and/or dental professionals where treatment is sought outside the UK.

Patients have the right of access to their health records held on paper or on computer. A request from a patient to see records or for a copy must be referred to the patient's dentist. The patient should be given the opportunity of coming into the practice to discuss the records and will then be given a photocopy. Care should be taken to ensure that the individual seeking access is the patient in question and where necessary the practice will seek information from the patient to confirm identity. The copy of the record must be supplied within forty days of payment of the fee and receipt of identifying information if this is requested.

Why would a patient want to access their dental records?

The patient will have their own reason to request their dental records and they do not need to give a reason why when making a request.

Who can make a request?

A request to access dental records, or any part of the dental record, can be made by the following people:

- the patient
- a person authorised in writing to make the application on the patient's behalf
- A person having parental or guardian responsibility for the patient
- where the patient is incapable of managing his own affairs, any person appointed by a court to manage those affairs
- where the patient has died, the patient's personal representative and any person who may have a claim arising out of the patient's death.

Exemptions to Access

There are two main exemptions to a patient's right of access which are:

- information about identifiable third parties
- information likely to cause someone serious physical or mental harm

The first exemption means those who hold the information (known as data controllers in the legislation) may refuse to release it if it would reveal information about another person unless that person has given consent.

The second exemption means that access can be refused if it is likely to cause serious harm to the physical or mental health or condition of the data subject or any other person. The term "any other person" could relate to a health professional or a relative of the patient. Subject access rights can be refused if it was considered likely to put a health professional or a family of the patient in danger.

Access to Dental Records - Patient Fees

Under the Data Protection Act 1998 (Fees and Miscellaneous Provisions) Regulations 2001, patient charges apply.

The patient can be charged for **copies** as follows:

- £10 if dental records and radiographs held on computer
- £50 if the dental records and radiographs held in part on computer and in part manually or are all manual

The patient can be charged to **view only** (no copies made) their records as follows:

- £10 if dental records are held totally on computer
- £10 if the dental records are held manually or are in part held manually and on computer

If a person wishes to view their health records and then wants to be provided with copies this would still come under the one access request. The £10 maximum fee for viewing would be included within the £50 maximum fee for copies of health records, held in part on computer and in part manually.

Requests to access dental records of a deceased person

Access to the health records of a deceased person is governed by the Access to Health Records Act 1990. You will only be able to accept requests under the following circumstances:

- next of kin or legal executor
- permission of the next of kin
- have written permission from the deceased person given before they died.

Dental Record Requests for Treatment Outside the UK

Should a request be made by a patient who is seeking dental treatment outside the UK, the legal right to access dental records and radiographs is the same as given in the above. Patients do not have to give a reason why are requesting a copy of their dental records and it is under their own action and consent that they are disclosing personal information to a dental professional abroad.

For former patients living outside of the UK, but who have undergone treatment while living in the UK still have the same rights to apply for access to their UK dental records. Such requests should be dealt with as someone making an access request from within the UK.

Original health records should not be given to patients to keep/take to a new dentist outside the UK. The Department of Health recommend that original patient health records should not be sent to patients or their authorised representative because of the potential detriment to patients should the records be lost and for medico-legal purposes.

For further sources of information please visit: www.ico.gov.uk or seek advice from your legal representative should you be concerned about a particular case or exemption issues.

General Rules

The fact that patients have the right of access to their records makes it essential that information is properly recorded. Records must be:

- contemporaneous and dated
- accurate and comprehensive

- signed by the dentist
- neat, legible and written in ink
- strictly necessary for the purpose
- not derogatory
- such that disclosure to the patient would be unproblematic.

Practical rules

The principles of confidentiality give rise to a number of practice rules that everyone in the practice must observe:

- records must be kept secure and in a location where it is not possible for other patients or individuals to read them
- identifiable information about patients should not be discussed with anyone outside of the practice including relatives or friends
- a school should not be given information about whether a child attended for an appointment on a particular day. It should be suggested that the child is asked to obtain the dentist's signature on his or her appointment card to signify attendance
- demonstrations of the practice's administrative/computer systems should not involve actual patient information
- when talking to a patient on the telephone or in person in a public area care should be taken that sensitive information is not overheard by other patients
- do not provide information about a patient's appointment record to a patient's employer
- messages about a patient's care should not be left with third parties or left on answering machines. A message to call the practice is all that can be left
- recall cards and other personal information must be sent in an envelope
- disclosure of appointment books, record cards or other information should not be made to police officers or Inland Revenue officials unless upon the instructions of the dentist
- patients should not be able to see information contained in appointment books, day sheets or computer screens
- discussions about patients should not take place in public areas of the practice.

Disciplinary action

If, after investigation, a member of staff is found to have breached patient confidentiality or this policy, he or she shall be liable to summary dismissal in accordance with the practice's disciplinary policy.

Employees are reminded that all personal data processed at the practice must by law remain confidential after your employment has terminated. It is an offence under section 55(1) of the Data Protection Act 1998, knowingly or recklessly, without the consent of the data controller [**Christian Gollings**], to obtain or disclose personal data. If the practice suspects that you have committed such an offence, it will contact the Office of the Information Commissioner and you may be prosecuted by the Commissioner or by or with the consent of the Director of Public Prosecutions.

A **Subject Access Request (SAR)** may be made not only by the individual but also by third parties on behalf of that individual.

The following guidance covers the information required before a request can be met.

- **Subject Access Request – By the Individual** (i.e. the living individual, to whom records refer and who is making the request). On the submission of a written request, and verification of identity (i.e. confirmation that the person requesting the records is the data subject) access is permitted by the data subject to all their medical/dental records in accordance with the act.

- **Subject Access Request – By a Third Party** (i.e. on behalf of a living individual who is incapable of managing his/her affairs, any person appointed by the court to manage those affairs, or persons interested in an individual's medical/ dental records). Before medical/dental records can be disclosed, the written consent of the individual is required. In circumstances where individuals are incapable of managing their own affairs the consent for disclosure must be obtained from the appropriate authority.

Access to any part of a health record can be refused if:

- In the written opinion of the health professional, acting on behalf of the data controller, disclosure of the records would be likely to cause serious harm to the physical or mental health of the individual (data subject) or any other person.

- Information relating to or provided by someone other than the data subject could identify that individual.

- Unless that individual is a health professional who has compiled or contributed to the health record or has been involved in the treatment of the data subject
- Unless that individual has given their consent to the disclosure of the information to the person making the request.
- Unless it is reasonable in all the circumstances to comply with the request without the consent of the other individual.

A person other than the data subject is making the request for access on behalf of the individual (data subject) e.g. a person with parental responsibilities for the data subject or a person appointed by the court to manage the affairs of the data subject and the data subject:

- provided that the information in the expectation that it would not be disclosed to the person making the request.
- consented to any examination or investigation in the expectation that the information would not so be disclosed;
- has expressly indicated that the information should not be disclosed.

Data Subjects must submit a written request and forward it to the DPO.

The DPO has 40 calendar days from receipt of a SAR to respond to a request. Any longer period will be a breach of the Act. Speed of handling is therefore essential. A request from a patient to see records or for a copy must be referred to the patient's dentist. The patient should be given the opportunity of coming into the practice to discuss the records and will then be given a photocopy.

Data Protection Principles

The eight Data Protection Principles as laid down in the 1998 Data Protection Act (along with Caldicott Principles) must be followed at all times:

1. Data must be processed fairly and lawfully
2. Personal data shall be obtained only for one or more specific and lawful purposes
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose for which they are processed.
4. Personal data shall be accurate and where necessary kept up to date.
5. Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose.
6. Personal data shall be processed in accordance with the rights of data subjects under the 1998 Data Protection Act

7. 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. Personal data shall not be transferred to a country outside the EEA, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

The Caldicott Principles

Principle 1 - Justify the purpose(s)

Every proposed use or transfer of patient-identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed by an appropriate guardian.

Principle 2 – Don't use patient-identifiable information unless it is absolutely necessary

Patient-identifiable information items should not be used unless there is no alternative.

Principle 3 – Use the minimum necessary patient-identifiable information

Where use of patient-identifiable information is considered to be essential, each individual item of information should be justified with the aim of reducing identifiably.

Principle 4 – Access to patient-identifiable information should be on a strict need to know basis.

Only those individuals who need access to patient-identifiable information should have access to it, and they should only have access to the information items that they need to see.

Principle 5 – Everyone should be aware of their responsibilities

Action should be taken to ensure that those handling patient-identifiable information – both clinical and non-clinical staff – are aware of their responsibilities and obligations to respect patient confidentiality

Principle 6 – Understand and comply with the law.

Every use of patient-identifiable information must be lawful. Someone in the practice should be responsible for ensuring that the practice complies with legal requirements.

Responsible Person

Christian Gollings have been appointed to be the person responsible for Confidentiality.

Training

Training on Confidentiality should be carried out at least annually and recorded in Individual's CPD Portfolios.

More information

For more information on this topic, speak with the Practice Owners or Administration Manager. Alternatively contact the organisations below.

General Dental Council (www.gdc-uk.org)

Information Commissioner (www.informationcommissioner.gov.uk)

Dental Defence Union (www.the-ddu.com)

Dental Protection Ltd (www.dentalprotection.org)

MDDUS (http://www.mddus.com/)

Approval

This policy has been approved by the undersigned and will be reviewed on an annual basis.

Name:	**Julie Williams (IG Lead) Christian Gollings (Practice Owner)**
Date:	**12 Jan 2018**
Previous Policy Update Dates:	12 Oct 2017; 09 June 2017**;** 10th March 2016
Signed:	CAG, CLG, LS, LW, JW, LD
Next Review Date:	**2019**