# 

# Data Protection Policy

* This practice will ensure data is kept secured from unauthorised access.
* There is no discussion of confidential, person identifiable information with, or disclosure to, a third party without explicit agreement of the Registered Manager.
* Transfer of data between cooperating service providers is timely for patient care purposes, sufficient for service provision, restricted to relevant material, and safely transferred.
* Office is compliant with the General Dental Council's publication, 'Standards of the Dental Team (2013)' and 'Principles of Confidentiality'. All team members are trained to know and follow these requirements.
* There is advice on assessing a Patients mental capacity in the Mental Capacity Act 2005 - Codes of Practice.
* The team is aware of their responsibilities regarding confidential data and will sign a written statement (contained in their contract of employment) about their responsibilities to maintain data protection at all times.
* Information Governance Lead (may also be known as a Caldicott Guardian) will manage, audit and record observation of current practices and procedures when dealing with confidential information.

# Procedure

* Treat information about patients as confidential and only use it for the purposes for which it is given.
* Prevent information from being accidentally revealed and prevent unauthorised access by keeping information secure at all times.
* In exceptional circumstances, it may be justified to make confidential Patient information known without consent if it is in the public interest, for example if requested by police.
* Any breach of confidence will be reported to the relevant professional bodies to be investigated.
* Limited Reasons for disclosure are:
  + With the written agreement of the Patient, for insurance purposes or when involved in a complaint
  + On referral to another Provider
  + In the wider Public Interest, involving serious risk to the public or serious crime
  + By Court Order, but only the minimum required to comply
* No records will be left, or used in a manner, where other Patients or visitors can access or read them.
* Suitable arrangements will be consistently in place for the safe destruction of confidential data.
* Information must remain confidential, detailed below are some specific examples of when NOT to disclose:
  + Request from a school about the attendance of a child
  + Request from a parent (unless sure of being Legal Guardian) about the attendance of a child
  + Request from a solicitor for information, or someone acting on behalf of a third party
  + Request from a family member, even a spouse, about the attendance of a Patient, or to discuss treatment

The following procedures must be followed to ensure a confidential and secure environment is maintained:

* There is a safe and private place for confidential discussions with a Patient
* Telephone conversations with, or about, a Patient cannot be overheard in the public areas
* All computers are password protected, and staff must `log out` when not sitting at a computer
* No unencrypted portable device is used to transfer or store data
* All postal contacts with Patients are in a plain sealed envelope

Patients have a right of access to their records. When requested copies must be produced within 40 days of receipt of a written request. A fee for this service may be charged, in line with Data Protection advice.