# Data Protection Policy

The practice is committed to complying with the Data Protection Act 1998 and the GDC Standards by collecting, holding, maintaining, and accessing data in an open and fair fashion.

The practice only keeps relevant information about employees for the purposes of employment, and about patients to provide them with safe and appropriate dental care. The practice does 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 are also kept confidential.

Hard copy and computerised records are stored, reviewed, and updated securely and confidentially. Records are securely destroyed when no longer required. Confidential information is only seen by personnel who need to see it and the team are trained on our policies and procedures to keep patient information confidential.

To facilitate patients' health care, the personal information may be disclosed to a doctor, health care professional, hospital, NHS authorities, HMRC, the Benefits Agency (when claiming exemption or remission from NHS charges) or private dental schemes of which the patient is a member. In all cases only relevant is shared. In very limited cases, such as for identification purposes, or if required by law, information may have to be shared with a party not involved in the patient's health care. In all other cases, information is not disclosed to such a third party without the patient's written authority.

All confidential information is sent via secure methods. Electronic communications and stored data are encrypted. All computerised clinical records are backed up and encrypted copies are kept off-site. No information or comments about patients are posted on social networking or blogging sites. Criminal record check information is kept securely in a lockable, non-portable storage cabinet with access strictly controlled and limited to persons who need to have access to this information in the course of their duties.

**Data Breach**

The practice will report serious data breaches to the ICO within 24 hours of becoming aware of the essential facts. The practice will keep a log of all personal data breaches and record the basic facts, effects of the breach and remedial action taken.

**Access to records**

Patients and team members can have access to view the original of their records free of charge. Copies of patient or team member records are provided following a written request to the Practice Manager, using the ICO Subject access request template, together with a payment of £10 for a copy of computerised records or £25 for a copy of paper records. X-ray copies are charged at the current cost of taking x-rays at the practice. The requested copies will be provided within 40 days on receipt of payment. An employee or a patient may challenge information held on record and, following investigation, should the information be inaccurate the practice will correct the records and inform person of the change in writing.

When the request for information is about the personal data of a child, the practice will consider if the child is mature enough to understand their rights. If they do, then the practice will consider responding directly to the child rather than the parent. When it is decided that the child is not mature enough to understand their rights, and there is some doubt about parental responsibility, proof of identity and evidence of parental responsibility will be requested (See M 216).

When the practice receives a third-party request for information on someone else's behalf (e.g. from a solicitor) evidence of their permission will be requested, this could be a written authority to make a request or a power of attorney.

When the practice receives a third-party request for information for a patient who lacks the mental capacity to manage their affairs the practice will ask to see evidence of a Lasting Power of Attorney or the evidence of appointment by:

- The Court of Protection in England & Wales
- The Sheriff Court in Scotland and
- The High Court (Office of Care and Protection) in Northern Ireland

This policy should be read in conjunction with the Confidentiality Policy, and the Information Governance Procedure