Privacy Statement

This privacy policy sets out how the Hook Services ltd uses and protects any information that you give when you use this website. The company is committed to complying with the;

- Data Protection Act 1998, the General;
- Data Protection Regulation (GDPR);
- General Dental Council (GDC);
- and other standards.

The Hook Services ltd only keeps relevant information about doctors and patients to provide them with safe and appropriate services.
The person responsible for Data Protection in the Hook Services ltd is Korosh Majidi.
Our legal basis for processing data is:

- Consent
- Processing is necessary for the performance of our care for patients
- And the health care data we process is called special data, our legal basis for processing it is:
    - "9(2)(h) – Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional."

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 dentist, doctor, health care professional, hospital, or private dental schemes of which the patient is a member. In all cases only relevant information 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 never 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 company has appropriate procedures to ensure personal data breaches are detected, reported and investigated effectively, including procedures to assess and then report any breaches to the ICO where the individual is likely to suffer some form of damage, e.g. through identity theft or confidentiality 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.

Subject Access Requests
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 Korosh Majidi using the ICO Subject access request template, together with a payment of £50 for a copy of computerised records. 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 the person of the change in writing.
When the request for information is about the personal data of a child, the company will consider if the child is mature enough to understand their rights. If they do, then the company will consider responding directly to the child rather than the parent. If 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. The practice will update its privacy notice to ensure its gives information in a language that can be understood by a child on any processing of children's personal data.
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;

This policy should be read in conjunction with the Confidentiality Policy (M 233-CON), and the Information Governance Procedure (M 217C).

Consent for Marketing
When we obtain consent for marketing such as email marketing, this consent is specific, granular, clear, prominent, opt-in, documented and easily withdrawn. We have a system used to record consent and implement appropriate mechanisms in order to ensure an effective audit trail.

Deleting Personal Data
Our procedures for deleting personal data in electronic or paper format are detailed in the Record Management Policy (M 233-REM). If not related to necessary clinical or employment records we will delete personal data.