Confidentiality Policy

The practice is committed to complying with the requirements of the legislation governing patient confidentiality including: Access to Health Records 1990, Caldicott Guidelines 1997 - see the Data Quality Policy (M233-DPQ), Confidentiality Code of Practice 1998, Data Protection Act 2018, GDPR and the current GDC Standards.

For the purpose of this policy, confidential information is defined as all the information that is learnt in a professional role including personal details, medical history, what treatment a patient is having and how much it costs. The definition of personal details includes, but is not limited by, such details as name, age, address, personal circumstances, race, health, sex and sexual orientation, etc. Note that even the fact that a patient attends the practice is confidential. Confidential information may be supplied or stored on any medium including images, videos, health records, and computer records or may be transmitted verbally.

All staff members must be aware of their responsibilities for safeguarding patient confidentiality and keeping information secure and must have received appropriate training on the legislation requirements and the current GDC Standards to ensure that:

- No personal information given or received in confidence is passed on to anyone else without the patient's prior consent. To obtain consent a patient is advised what information will be released and why and the likely consequences of the information release. The patient is given an opportunity to withhold their permission to share information, unless exceptional circumstances apply, and note is made on their clinical record of whether or not they gave their permission

- If a patient consents to sharing information about them the team member will ensure that all recipients of the information understand that it is confidential. When referring to dental or medical colleagues we expect them to have the same high standards

- If a patient's information or images are used for research or marketing the team member will advise the patient how these will be used, check that the patient understands what s/he is agreeing to, obtain and record the patient's consent to their use and only release the minimum information for the purpose. The patient will be advised that s/he can withdraw permission at any time

- If it is not necessary for a patient to be identified, they will remain anonymous in any information released

- The duty to keep information confidential also covers originals and copies of a patient's photographs, videos or audio recordings, including those made on a mobile phone. No images or recordings will be made without the patient's permission

- Patient information is kept confidential even after death

Before releasing information without the patient's permission, an effort is always made to either convince the patient to release the information himself or herself or give the practice permission to do so, with the details of the discussion fully documented in the patient record. If obtaining consent from a patient is not practical or appropriate or if the patient will not give their permission, the team member will obtain advice from their professional indemnity organisation before releasing it.

A patient's information will only be released without their prior permission in the following exceptional circumstances:

- It is in the best interests of the public or the patient and the information released could be important in preventing or detecting a serious crime
- If a team member has information that a patient could be at risk of significant harm or may be a victim of abuse, in which case the appropriate care agencies or the police will be informed
- If a team member is required to disclose information by a court or a court order, in which case only the minimum amount of information necessary to comply will be released

The practice treats breaches of confidentiality very seriously. No team member shall knowingly misuse any confidential information or allow others to do so. Failure to comply with this policy may result in disciplinary action.

This policy should be read in conjunction with the Social Media Policy (M 233-SMD), Data Quality Policy (M233-DPT), Information Protection and Security Policy (M 233-DPT) and the Information Governance Procedures (M 217C).