ACCESSIBLE ORTHODONTICS

DATA PROTECTION POLICY

Date adopted: 18 / 05 / 2018
For Review: **AUG** yrly

The purpose of our Data Protection Policy is to support the 7 Caldicott Principles, the 10 Data Security Standards, the General Data Protection Regulation (2016/679) (as amended by UK law, from time to time) ("**GDPR**"), the Data Protection Act 2018 (if applicable), the Human Rights Act 1998, the common law duty of confidentiality and all other relevant national legislation. We recognise Data Protection as a fundamental right and embrace the Principles of **Data Protection by design and by default**.

The Practice is committed to collecting, holding, maintaining and accessing data for a lawful purpose and in a secure environment. As a result we will adhere to our duty of candour responsibilities as outlined in the Health and Social Care Act 2012 and adopt Policies in keeping with that commitment.

This Policy includes in its scope all data which we processeither in hardcopy or digital copy, this includes special categories of data. It applies to all staff, including temporary staff and contractors. Members of our Team support our commitment to Data Protection by undertaking regular training and, if applicable, special learning, as idneitifed in our Training Needs Assessment.

Data Purpose

The Practice will only obtain, process and keep personal data / information for a lawful purpose. That means:

◊ of Patients / Service Users – for the purpose of providing them with dental care

◊ of Team Members - for the purposes of employment.

Data Subjects - their Data & their Rights

The Practice will be open and transparent with Service Users and those who lawfully act on their behalf in relation to their care and treatment.

We will not process any relevant 'special category data' unless it is legally entitled to OR it has prior informed consent. As defined by GDPR &/or the Act "**special category 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 will be kept confidential.

Any personal data collected will be specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Care is taken to ensure that data will be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')

We need to keep comprehensive and accurate personal data about our Patients to provide them with safe and appropriate dental care. We also need to process personal data about Patients in order to provide care under NHS arrangements and to ensure the proper management and administration of the NHS. All manual and computerised records will be kept in a secure place: they will be reviewed regularly, updated and destroyed in a confidential manner when no longer required. Personnel records will only be seen by appropriate management.

Patients' records will only be seen by appropriate Team Members. To facilitate Patients' health care the personal information about them may be disclosed to a doctor, health care professional, hospital, NHS authorities, the HM Revenue & Customs, the Department for Work and Pensions and its agencies (when claiming exemption or remission from NHS charges) or private dental schemes of which the Patient is a member. In all cases the information shared will be only that which is relevant to the situation. 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 will not be disclosed to such a third party without the Patient's written authority.

We will establish and maintain Policies for the controlled and appropriate sharing of service user and staff information with other agencies, taking account all relevant legislation and Subject consent.

In keeping with our commitment to transparency and proper data protection we will provide Patients and Team Members with a copy of our relevant Privacy Notice early in our relationship.

We uphold the personal data rights outlined in the GDPR and will develop, maintain and use Procedures which ensure we respond approiately to a Subject's exercise of thier rights.

All requests to exercise a Data Subject's Rights will be recorded immediately and accurately. We will respond appropriately and as required by law to requests by a Data Subject to exercise their rights.

So long as we are assured of their identity we will give them access to their own records. If they indicate changes are needed to keep them accurate we will do so immediately. Copies of their records, if sought, will be provided as required by law (including in a portable format).

Any request to not record or otherwise process personal data will be seriously considered. If we identify that compliance with the request will compromise the delivery of proper treatment to a Patient or could/would cause us to act unlawfully we will explain those consequences and act in accordance with our views if the request is insisted upon.

Requests to delete personal data will only be complied with if doing so will not compromise our legal obligations (owed to the Data Subject, or otherwise)

In line with legislation we engage or employ a Data Protection Officer (DPO) who will report to the highest management level of the organisation. We will support the DPO with the necessary resources to carry out their tasks and ensure that they can maintain expertise. We guarantee that the DPO will not be pressured on how to carry out their tasks and that they are protected from disciplinary action when carrying out the tasks associated with their role.

We will undertake annual audits of our compliance with legal requirements.

Data protection by design & by default

We will undertake annual audits of our compliance with legal requirements.

We shall implement appropriate organisational and technical measures to uphold the principles outlined above. We will integrate necessary safeguards to any data processing to meet regulatory requirements and to protect individual's data rights. This implementation will consider the nature, scope, purpose and context of any processing and the risks to the rights and freedoms of individuals caused by the processing.

We shall uphold the Principles of data protection **by design and by default** from the beginning of any data processing and during the planning and implementation of any new data process.

All existing data processing has been recorded on our Record of Processing Activities. Each process has been risk assessed and is reviewed annually.

We ensure that, by default, personal data is only processed when necessary for specific purposes and that individuals are therefore protected against privacy risks.

In all processing of personal data, we use the least amount of identifiable data necessary to complete the work it is required for. Where any of the Data is to be processed for a purpose ancillary to the stated Data Purpose (above) prior, express Consent will be obtained from the Data Subject. In addition techniques of *anonymisation* or *pseudonymisation* will be used as a further way to give effect to ' data minimisation'.

We only keep the information for as long as it is required for the purposes of processing or any other legal requirement to retain it.

Any new high-risk data processing activities will be assessed using a Data Privacy Impact Assessment (DPIA) before the processing commences.

All new systems used for data processing will have Data Protection built in from the beginning of the system change.

Suite of inter-dependant, supporting Policies

Our suite of Policies (and their related Procedures) which support and inform our behaviour in the area of Data Protection contains:

◊ **Data Quality Policy** – outlines procedures to ensure the accuracy of records and the correction of errors

◊ **Data Security Policy** – outlines procedures for the ensuring the security of data including the reporting of any data security breach

◊ **Record Keeping Policy / Records Management and Security Policy** – details transparency Procedures, the management of records from creation to disposal (inclusive of retention and disposal procedures), information handling Procedures, Procedures for subject access requests, right to erasure, right to restrict processing, right to object, and withdrawal of consent to share

◊ **Network Security Policy** – outlines Procedures for securing our network

◊ **Staff Confidentiality Code of Conduct** - provides staff with clear guidance on the disclosure of personal information

◊ **Business Continuity Plan** –outlines the procedures in various circumstances, including in the event of a security failure or disaster affecting digital systems or mass loss of hardcopy information necessary for the day to day running of our organisation