Apple Dental Ceramics Ltd.

(For the purposes of this document known as the "Company")

LABORATORY CONFIDENTIALITY & DATA PROTECTION POLICIES

Confidentiality

The need for the strict confidentiality of personal information about patients and clients is taken very seriously. This document sets out our policy for maintaining confidentiality and all members of the laboratory team must comply with these safeguards as part of their contract of employment.

The importance of confidentiality

The relationship between the Company and our clients is based on the understanding that any information received regarding a patient will not be divulged without prior consent. Patients undergoing dental treatment have the right to privacy and this is extended to information supplied by the dentist to the Company. If confidentiality is breached, the Dental Care Professional (DCP) faces investigation by the General Dental Council and possible erasure from the DCP Register.

All staff must follow the General Dental Council's rules for maintaining patient confidentiality contained in *Standards for dental professionals* and *Principles of patient confidentiality*.

If confidentiality is breached, each registered dental professional involved is responsible to the Council for their individual conduct.

Personal information

In a dental laboratory context, personal information held by the Company about a patient may include:

- the patient's name, gender, shade of teeth and age
- information about the type of dental appliance required

Principles of confidentiality

The Company has adopted the following principles of confidentiality:

Personal information about a patient and our clients:

- is confidential in respect of that patient and to those providing the patient with health care should only be disclosed to those who would be unable to provide effective care and treatment without that information (*the need-to-know concept*), and such information should not be disclosed to third parties without the consent of the patient except in certain specific circumstances described in this policy.

Disclosures to third parties

There are certain restricted circumstances in which the Company may decide to disclose information to a third party or may be required to disclose by law. A brief summary of the circumstances is given below.

When disclosure is in the public interest

There are certain circumstances where the wider public interest outweighs the rights of the patient to confidentiality. This might include cases where disclosure would prevent a serious future risk to the public or assist in the prevention or prosecution of serious crime.

When disclosure can be made

There are circumstances when personal information can be disclosed:

- where expressly the patient has given consent to the disclosure
- where disclosure is necessary for the purpose of enabling someone else to provide health care to the patient and the patient has consented to this sharing of information
- where disclosure is required by statute or is ordered by a court of law
- where disclosure is necessary for the Company to pursue a bona-fide legal claim against a patient or client, when disclosure to a solicitor, court or debt collecting agency may be necessary.

DATA PROTECTION POLICY

Keeping records

Due to the nature of records held by the Company, registration with the Information Commissioner is not required.

What information do we hold?

To provide our clients and their patients with dental appliances the information held by the Company to enable manufacture of the appliance and invoicing activities includes:

- Patient name or in it's absence a reference number and on occasion's details such as age and gender should this be necessary to produce the appliance.
- Study models and where necessary clinical photographs and digital scans.
- Information about the required design of the dental appliance.
- Information about the dental practice.

Why do we hold this information?

To enable our business to undertake proper accounts and to maintain compliance with the Medicines and Healthcare product's Regulatory Agency (MHRA).

Processing data

No data is processed in this laboratory expect for producing financial invoicing to our clients.

DATA SECURITY POLICY

This laboratory is committed to ensuring the security of all data and information held by the business and this objective is expected by every member of our team without exception.

Confidentiality

- All staff employment contracts contain a confidentiality clause.
- Access to any information held is on a "need to know" basis only. Access to information is monitored and breaches of security will be dealt with swiftly.

Physical security measures

- Records are kept in a lockable fireproof cabinet, which is not easily accessible by visitors to the laboratory.
- Efforts have been made to secure the laboratory against theft by, for example, the use of intruder alarms, lockable windows and doors.
- The laboratory has in place a business continuity plan in case of a disaster. This includes procedures set out for restoring data.

Information held on computer

- Appropriate software controls are used to protect computerised records, for example the use of passwords and encryption. Passwords are only known to those who require access to the information, are changed on a regular basis and are not written down or kept near or on the computer for others to see
- Regular back-ups of computerised data are taken and stored off-site. Back-ups are also tested at prescribed intervals to ensure that the information being stored is usable should it be needed
- Staff using computers will undertake computer training to avoid unintentional deletion or corruption of information
- Precautions are taken to avoid loss of data through the introduction of computer viruses

CLOSED CIRCUIT TELEVISION (CCTV)

CCTV is in use within our premises, images are treated as "data" in the same manner as paper or computer based information. The main purpose of collecting data from CCTV cameras is the protection of Company employees and the public, the prevention of crime or anti-social behaviour and to safeguard Company property.

Data from CCTV cameras may be used as evidence during criminal or other legal proceedings and may be passed to other agencies within the scope of our Registration with the Information Commissioner.

The number and type of cameras has been carefully considered. Tenants, visitors and employees should not feel uncomfortable by the presence of CCTV and it will not be used to monitor private areas such as inside an office etc. It should also be noted that cameras may not always be immediately visible to the casual observer.

A senior member of staff is responsible for ensuring that those on site are aware of our DP Policy, the proper use of the system and how to respond to requests for access to recorded data.

Monitoring and Recording

Systems in use at the Company will not be monitored on a constant basis. Employees may check the system from time to time, for example to see who is at the door. Employees should not use the system for monitoring movements of people in and around the scheme. They would not be expected to respond to requests from other tenants who, for example, may want to find out what time someone went out or came back into the scheme.

The CCTV monitor should not be in a position where images can be seen by members of the public. If a meeting is being conducted in an office where CCTV is monitored, the CCTV monitor should be switched off if there is a risk that unauthorised people would be able to view images on screen.

Images will be recorded on a time loop. This means that recorded images are not kept indefinitely and will be recorded over on a regular basis. The length of time images are stored before being overwritten is 10 days.

Recorded images are kept securely and only accessible for specific purposes related to the use of CCTV, i.e. crime prevention/detection or dealing with anti-social behaviour.

CCTV images are the property of the Company as the Data Controller.

Notification

It is the responsibility of the Company to ensure that proper warning signs are sited in all areas covered by CCTV.

The sign should detail the purpose of using CCTV, who is responsible for operating the system and who to contact in the event of an enquiry.

This statement is available on the Company website and has been issued to all staff, clients and suppliers of the Company. Any concerns about the security of any information or data held should be addressed to a director of the Company.