PRACTICE INFORMATION SECURITY POLICY

This Dental Practice is committed to ensuring the security of personal data held by the practice. This objective is achieved by every member of the practice team complying with this policy. Other policy's that should be viewed with this are the practice Data Protection Policy and Data Confidentiality Policy.

Confidentiality (see also the practice confidentiality policy)

- All employed staff and contractor contracts contain a confidentiality clause.
- Access to personal data is on a "need to know" basis only. Access to information is monitored and breaches of security will be dealt with swiftly by the practice manager.
- We have procedures in place to ensure that personal data is regularly reviewed, updated and deleted in a confidential manner when no longer required. For example, we keep patient records for at least 11 years or until the patient is aged 25 – whichever is the longer.

Physical security measures

- Personal data including that held on digital media is only taken away from the practice premises in exceptional circumstances and when authorised by the Practice Manager or Principal Dentist. If personal data is taken from the premises it must never be left unattended in a car or in a public place. The one exception to this is computer backup data which is removed every night, the backup data is encrypted and password protected and never left unattended. Lab work is only to be giving to know employee of the lab directly in the form of a pickup from the lab, or a prearranged drop off to the lab and again given in person.
- Records, and computer back ups are kept in a lockable office which is not easily accessible to the public, or visitors to the practice, hard copy data is stored in a lockable fire resistant container.
- Efforts have been made to secure the practice against theft by, for example, the use of intruder alarms, lockable windows and doors.
- The practice has in place a business continuity plan in case of a disaster. This includes procedures set out for protecting and restoring personal data.

Information held on computer

- This practice is registered with the Information Commissioners office, a legal requirement of all organisations that process personal data.
- Appropriate software controls are used to protect computerised records, for example access to the computer system which stores patient records is individually password protected. 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.
- Daily and weekly back-ups of computerised data are taken and stored securely 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 practice computers will undertake in-house computer training at induction to avoid unintentional deletion or corruption of information.

- Dental computer systems all have a full audit trail facility preventing the erasure or overwriting of data. The system records details of any amendments made to data, who made them and when.

- The practice has up-to-date computer virus and firewall protection. We also employ specialist software and hardware support companies.

- Instant messaging software is not permitted in this surgery to avoid the risk of card details being transmitted to other locations, Mobile phones or memory sticks are also not permitted in the reception area. Without the express permission of the practice manager

- Computer hard disks and other media that store confidential patient and staff data including memory sticks will be disposed of in the following way. Please also read the practice acceptable use policy for internet computers and email,

    - The damaged or (otherwise not needed) disk should be passed to The practice manager
    - The practice manager will then run the hard disk through the acronis drive cleanser software. If this is not possible e.g. where the disk is inoperable the practice manager will physically destroy the disk portion of the hard disk.
- All of the physical media noted in appendix 1 that contains sensitive data is not allowed of the premises unless expressly authorised by the practice manager

Protection of Cardholder Data

- This practice complies with the PCI Data Security Standard. This standard aims to protect the data processed when patients pay by credit or debit card. An outline of the main points is noted below.

- Full card details will not be stored.

- Card validation codes and pin numbers will never be stored

- We only retain receipt information from card transactions, and these are marked as confidential.

- Should documents containing personal data need to be sent away, for example to the accountant for business reasons, they will either be delivered personally or via secured courier so that they can be tracked.

- Should personal information be sent via email for example to a referral dentist, they will be marked as restricted and to a specific named person, they will also request that the information is dealt with accordingly.

- Staff have been made aware not to let anyone touch the PDQ machine without express permission from BS this included service engineers for example.

- All data protection policies and procedures are subject to a yearly review, or a review when substantive changes to the business or the environment have occurred.

- The PDQ machine will be inspected at the start of each day for visible signs of tampering, and such signs noted will communicated to the practice manager. Once a month the PDQ will be checked by BS on the workplace inspections and logged.

This statement has been issued to existing staff with access to personal data at the practice and will be given to new staff during induction. Should any staff have concerns about the security of personal data within the practice they should contact The Practice Manager or the Principle Dentist.

Document History
This document created on the: 3rd March 2006

- Reviewed: 10th March 2006 No changes
- Reviewed 1st March 2007 No changes
- Reviewed 3rd April 2008 No changes
- Reviewed 18th Aug 2009: Added the Protection of card holder data section for compliance with the PCI. Added Information commission registration
- Reviewed 20 Aug 2010 No changes
- Reviewed 26th Sep 2011 Added the restriction on instant messaging and mobile phone restrictions service on reception computer, added the procedure for deleting data from unwanted storage media.
- Reviewed 9th sep 2012 added link to the acceptable use policy that has been developed
- Reviewed July 2013 no change
- Reviewed Sep 2013 No change
- Reviewed Oct 2014 No change BS
- Reviewed Jan 2016 No Change MA
- Reviewed April 2017 added appendix 1and other changes in response to new PCI questionnaire.BS
- Reviewed Jan 2019 No changes
- Reviewed Jan 2020 no changes
- Reviewed Feb 2021 No changes

Appendix 1 list of active electronic and paper media that may be used for collection and use of peoples personal data, and the authorisation of staff to use them.

Item	Identification	Location	Nature of data	Authorised to use
Acer PC		Reception	Clinical, personal	All TNS Staff, and VA
Incognito PDQ		Reception	Financial, personal	AN, BS, TN, JC
Acer PC		S2	Clinical, personal	All TNS staff and VA
Acer PC		Office	Clinical personal	All TNS staff and VA GE
HP Microserver		Office	Clinical Personal	ONLY BS
5 seagate backup disks		Office, Home	Clinical, personal	BS, NB
Acer PC		S1	Clinical personal	All TNS staff and VA
Hudl 2 tablet computer		Various,	Clinical personal	All TNS staff and VA
Physical files containing past payment transactions and mpan numbers		Cupboard under the stairs in the office	Financial	BS NB GE
Medical History files		Cupboard under the stairs in the office	Clinical personal	All TNS staff and VA
Lab work		Cupboard in the Decon room	clinical	JC TN AN NB BS