Data Security Policy

This policy is to be read in conjunction with the Data Protection Policy.

NR2 Dental Studio is required to safeguard the security of personal data held by the practice.

This objective is achieved by every practice team member, i.e., all company personnel, who comply with this policy.

Confidentiality (see also the practice confidentiality policy)

- All Company Personnel contracts and agreements contain a confidentiality clause.
- Access to personal data is only on a “need to know” basis. Access to information is monitored, security breaches will be handled seriously and swiftly, and you understand the Caldicott Principles.
- We have procedures to ensure that personal data is regularly reviewed, updated, and deleted confidentially when no longer required. For example, we keep patient records for at least 11 years or until the patient is 25 – whichever is longer.
- All staff will receive training during their induction period on the safe handling of data and how data is used, stored and shared within our practice.

Physical security measures

- Personal data is only taken from the practice premises in exceptional circumstances and when authorised by the DPO. No personal data is to be taken from the premises, and it must never be left unattended in a car or a public place.
- Records are to be kept in a lockable cabinet or locked/password-protected computer, which is not easily accessible by patients and visitors to the practice.
- Efforts have been made to secure the practice against theft by, for example, using intruder alarms, lockable windows, and doors that should remain locked at suitable times, particularly when leaving the practice at night.
- The practice has a business continuity plan in case of a disaster. This includes procedures set out for protecting and restoring personal data.
- The Information Asset Register (IAR) contains the location of all confidential information (Compliance Suite > GDPR > DSP Toolkit), and a risk assessment is completed to ensure it is adequately secured.

Information held on the computer

- Passwords are only known to those who require access to the information, are changed regularly and are not written down or kept near or on the computer for others to see.
- The Information Asset Register (IAR) contains the location of all confidential information that is stored digitally (Compliance Suite > GDPR > DSP Toolkit), and a risk assessment is completed to ensure it is adequately secured.
- Daily and weekly backups of computerised data are taken and stored off-site.
- Back-ups are also tested at prescribed intervals to ensure that the stored information is usable, should it be needed.
- Staff using practice computers will undertake computer training to avoid unintentional deletion or corruption of information.
- Dental computer systems all have a complete audit trail facility, preventing the erasure or overwriting of data. The system records any amendments made to data, who made them and when.
- Precautions are taken to avoid loss of data through the introduction of computer viruses.
- When a staff member leaves, their access to the computer systems will be revoked.

This statement has been issued to Company Personnel, including all employees, associates, hygienists, and, without limitation, other self-employed staff, workers, contractors, agency workers, consultants, directors, members, and others who have 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 DPO or the practice manager.

Cyber Security

Core cyber security principles:

Access Control:

- Access controls are based on job roles, and only authorised personnel should have access to patient data.
- User accounts must be protected by strong passwords
- Multi-factor authentication (MFA) is required for remote access and cloud-based services.
- User accounts are immediately removed or deactivated when a staff member leaves the practice.

Device Security

- All devices used within the practice, or remotely, must have anti-virus/malware protection.
- Devices must be encrypted and auto-lock when inactive for a period of time.

Email & Internet Usage

- Staff must be vigilant of phishing emails and suspicious links – training must be given to all staff on cyber security.
- Emails containing personal or patient information must be encrypted or sent via secure platforms such as NHSmail.

Data Handling

- Patient data must be stored on secure, encrypted systems
- Backups are done regularly and stored securely
- No patient data can be downloaded or stored on personal devices unless given prior authorisation.

Remote access – please see the Remote Access Policy

Data and Cyber Security Breach

In the event of a data breach, whether digital or physical records, or a suspected or actual cyber incident, such as phishing emails, lost devices or unauthorised access, the Practice Manager or DPO should be immediately informed. We will then follow our data breach/incident response plan (Compliance suite > GDPR > Data Breach Documentation)

The staff member who discovers the breach or cyber security incident should promptly complete a data breach form. They should then inform the Practice Manager and/or the DPO, who will investigate the breach. If it is felt that the breach is likely to affect the rights and freedoms of an individual, the ICO must be informed within 72 hours of the breach. If unsure whether a breach needs to be reported, there is a data breach self-assessment form on the DCME portal (Compliance Suite > GDPR > Data Breach Documentation).

Document Control

Title:	Data Security Policy
Author/s:	DCME Team

Owner:	DCME Team
Approver:	DCME Team
Date Original Approved:	02/05/24
Review Date:	July 2025
Next Review Date	July 2026

Change History				
Version	**Status**	**Date**	**Author / Editor**	**Details of Change** (Brief detailed summary of all updates/changes)
1.1	Final	02/05/24	DCME Team	Re-written policy
1.2	Final	07.2025	HD	Added information on cyber security, general grammar check and improvement.

The latest approved version of this document supersedes all other versions. Upon receipt of the latest approved version, all other versions should be destroyed, unless specifically stated that previous version(s) are to remain extant. If in any doubt, please get in touch with the document Author.

Approved By: Joana Lopes, Paulina Zamecka
Date Published: 17/07/2025