Data Security Policy

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

Lighthouse Dental Practice is required to safeguard the security of personal data held by the practice.

This objective is achieved by every member of the practice team, i.e. all Company Personnel complying 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, and breaches of security will be dealt with seriously and swiftly, and you understand the Caldicott Principles
- 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 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 in a public place.
- Records are to be kept in a lockable cabinet or locked/password-protected computer, which is not easily accessible by patients or 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 place 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 properly 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 properly 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 information being stored 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 details of 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.

Data Security Breach

In the event of a data breach, whether digital or physical records, our data breach procedures will be enforced.

The staff member who discovers the breach should promptly complete a data breach form. They should then inform 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 you are 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 Approved:	02/05/24
Next Review Date:	02/05/25

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
		10/5/24		Approved policy to go live

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 contact the document Author.

Approved By: Terri-Gail Phillips-Hale
Date Published: 10/05/2024