

The Dunhill Medical Trust (DMT)

Title: Compliance
Version: 1.1
Date: March 2018
To be reviewed: March 2019
Classification: Public

Introduction

This Compliance Policy is a sub-policy of the Information Security Policy and outlines the DMT's requirement to comply with certain legal and regulatory frameworks.

Compliance with legislation

The DMT provides policy statements and guidance for staff, Trustees and Committee members in relation to compliance with relevant legislation to help prevent breaches of the DMT's legal obligations. However, individuals are ultimately responsible for ensuring that they do not breach legal requirements during the course of their work.

Users of the DMT's online or network services are individually responsible for their activity and must be aware of the relevant legal requirements when using such services.

The DMT must comply with all relevant legal requirements whether such requirements are detailed in internal policies or not. Any suspected breach of the DMT's legal requirements must be reported to the Executive Director.

Software licence management

All software used for DMT business must be appropriately licensed. The DMT must comply with the software and data licensing agreements it has entered into. During the negotiation process of such agreements, full consideration must be given to how compliance with the agreement can practically be achieved. Agreements may need to be specifically negotiated to enable the DMT to comply.

Third party terms and conditions

Where the DMT uses the services of a third party provider, staff, Trustees and Committee members will also be subject to their terms and conditions in so far as they relate to information security.

Compliance with the DMT's Information Security Policy

The DMT's own information security policies must be adhered to at all times when handling DMT information and the DMT must ensure it is acting legally when operating such policies.

All staff, Trustees and other persons who may handle DMT information must be made aware of the DMT's information security policies and of any amendments made to them. Individuals must also confirm that they have read and understood these policies and how they apply to the information they handle.

Collection of evidence

At times, it may be necessary for the DMT to collect evidence in relation to a potential legal claim or internal investigation.

Where there is suspicion of a criminal offence involving the DMT's information or systems, the DMT will cooperate with the relevant agency to assist in the preservation and gathering of evidence on the basis of appropriate internal authorisation and compliance with relevant statutory requirements.

Records management

The DMT is required to retain certain information, whether held in hard copy or electronically, for legally defined periods. Such information must be appropriately safeguarded and not destroyed prior to the defined minimum retention period, while remaining accessible to those who require access and are authorised to access that information.

In accordance with the Data Protection Act (and its successor legislation), personal data should not be retained for longer than it is required for the purposes for which it was collected.