Title:	**Information Security Policy (Overarching)**
Version:	**1.0**
Date:	**March 2018**
Reviewed:	**March 2018**
To be reviewed:	**December 2020**
Classification:	**Public**

1. Introduction

This policy is concerned with the management and security of the DMT's information assets (an information asset is defined to be an item or body of information, an information storage system or an information processing system which is of value to the DMT) and the use made of these assets by its staff, Trustees, Committee members and others who may legitimately process DMT information on behalf of the DMT.

This overarching policy document provides an overview of information security and lists a hierarchical set of policy documents (sub-policies) which taken together constitute the Information Security Policy of the DMT.

2. Purpose

An effective Information Security Policy provides a sound basis for defining and regulating the management of information systems and other information assets. This is necessary to ensure that information is appropriately secured against the adverse effects of failures in confidentiality, integrity, availability and compliance which would otherwise occur.

3. Scope

The documents in the Information Security Policy set apply to all information assets which are owned by the DMT or used by the DMT for its legitimate business purposes. The documents in the Information Security Policy set apply to all information which the DMT processes, irrespective of ownership or form.

The documents in the Information Security Policy set apply to all staff, Trustees and Committee members of the DMT and any others who may process information on behalf of the DMT.

4. Information Security Principles

- Information will be protected in line with all relevant DMT policies and applicable legislation.
- Each information asset will have a nominated owner who will be assigned responsibility for defining the appropriate uses of the asset and ensuring that appropriate security measures are in place to protect the asset.
- Information will be made available solely to those who have a legitimate need for access.
- All information will be classified according to an appropriate level of security.
- The integrity of information will be maintained.
- It is the responsibility of all individuals who have been granted access to information to handle it appropriately in accordance with its classification.
- Information will be protected against unauthorised access.

- Compliance with the Information Security policy will be enforced.

5. Governance

Responsibility for the production, maintenance and communication of this top level policy document and all sub-policy documents lies with the DMT's Executive Director.

This top-level policy document has been approved by the Trustee Board of the DMT. Substantive changes may only be made with the further approval of the Board. Each of the documents constituting the Information Security Policy will be reviewed annually. It is the responsibility of the Executive Director to ensure that these reviews take place and that any changes are communicated.

6. Sub-Policy Document List

Compliance
Outsourcing and Third Party Compliance
Information Handling
Access and Password Management
Acceptable Use
Software Management
Mobile and Remote Working