Title:	Information Handling Policy
Version:	1.1
Date:	December 2020
Reviewed:	December 2020
To be reviewed:	December 2021
Classification:	Public

1. Introduction

This Information Handling Policy is a sub-policy of the Information Security Policy and sets out the requirements relating to the handling of the DMT's information assets. Information assets must be managed in order to protect against the consequences of breaches of confidentiality, loss of integrity, interruption to availability, and non-compliance with legislation which would otherwise occur.

2. Security classification

Each information asset will be assigned a security classification by the asset owner which reflects the sensitivity of the asset according to the following classification scheme:

Public - available to any member of the public without restriction.
Open - available to any authenticated member of the DMT.
Confidential - available only to specified members, with appropriate authorisation.
Strictly Confidential - available to only a very small number of members, with appropriate authorisation.
Secret - the most restricted category. It is not anticipated that many DMT assets will be assigned this classification.

Any information which is not explicitly classified will be classified as open, by default.

Any data which is classified as sensitive personal data under the EU General Data Protection Regulation will be classified as strictly confidential. Any data which is subject to the Official Secrets Act 1989 will be classified as secret.

3. Access to information

Staff, Trustees and Committee members of the DMT will be granted access to the information they need in order to fulfil their roles within the DMT. Individuals who have been granted access must not pass on information to others unless the others have also been granted access through appropriate authorisation.

4. Disposal of information

Great care needs to be taken to ensure that information assets are disposed of securely. Confidential paper waste must be rendered illegible before being disposed of.

Electronic information must be securely erased or otherwise rendered inaccessible prior to leaving the possession of the DMT, unless the disposal is undertaken under contract by an approved contractor.

In cases where a storage system (for example a computer disc) is required to be returned to a supplier it should be securely erased before being returned unless contractual

arrangements are in place with the supplier which guarantee the secure handling of the returned equipment. If this is not possible, then the storage system should not be returned to the supplier and should remain in the possession of the DMT until it is disposed of securely.

5. Removal of information
DMT data which is subject to the EU General Data Protection Regulation or which has a classification of confidential or above should be stored using DMT facilities or with third parties subject to a formal, written legal contract with the DMT, wherever possible. In cases where it is necessary to otherwise remove data from the DMT, appropriate security measures must be taken to protect the data from unauthorised disclosure or loss. Strictly confidential data in electronic form must be strongly encrypted prior to removal. Secret data must never be removed except with the explicit written permission of the data owner.

Particular care needs to be taken when information assets are in transit. Mobile devices used to access DMT assets must always be encrypted.

6. Using personally owned devices
Any processing or storage of DMT information using personally owned devices must be in compliance with the DMT's Mobile and Remote Working Policy.

7. Information on desks, screens and printers
Staff, Trustees and Committee members who handle confidential paper documents should take appropriate measures to protect against unauthorised disclosure, particularly when they are away from their desks. Confidential documents should be locked away overnight, at weekends and at other unattended times.

Care should also be taken when printing confidential documents to prevent unauthorised disclosure.

Computer screens on which confidential or sensitive information is processed or viewed should be sited in such a way that they cannot be viewed by unauthorised persons and all computers should be screen-locked while unattended.

8. Backups
Information owners must ensure that appropriate backup and system recovery measures are in place. Where backups are stored off site, appropriate security measures must be taken to protect against unauthorised disclosure or loss. Recovery procedures should be tested on a regular basis.

9. Exchanges of information
Whenever significant amounts of personal data or other confidential information are exchanged with other organisations, appropriate information security measures must be established to ensure the integrity and confidentiality of the data transferred. Regular exchanges must be covered by a formal written agreement with the third party.

Information classified as strictly confidential may only be exchanged electronically both within the DMT and in exchanges with third parties if the information is strongly encrypted prior to exchange. Information classified as secret may not be transmitted electronically except with the explicit written permission of the information owner. Hard copies of

information classified as strictly confidential or above must only be exchanged with third parties via secure (for example, special) delivery.

When exchanging information by email or fax, recipient addresses should be checked carefully prior to transmission.

Unsolicited emails, faxes, telephone calls, instant messages or any other communication requesting information which is not classified as public should not be acted upon until and unless the authenticity and validity of the communication has been verified.

Members of the DMT must not disclose nor copy any information classified as confidential or above unless they are authorised to do so.

10. Reporting losses

All members of the DMT have a duty to report the loss, suspected loss or unauthorised disclosure of any DMT information asset to the Executive Director.