

Title:	Acceptable Use Policy
Version:	1.1
Date:	December 2022
Reviewed:	December 2022
To be reviewed:	December 2023
Classification:	Public

1. Introduction

This Acceptable Use Policy is a sub-policy of the Information Security Policy and sets out the responsibilities and required behaviour of users of the DMT's information systems and devices used to access these systems by its staff and any other authorised individual (see Access and Password Management policy).

Each member of staff will also be assigned a unique email address for his or her individual use and some members may also be given authorisation to use one or more generic (role based) email addresses. Members must not use the email address assigned to anyone else without their explicit permission. Email addresses are DMT- owned assets and any use of these email addresses is subject to its policies.

2. Personal use of facilities

Personal use is permitted but only so long as:

- it does not interfere with the member of staff's work
- it does not contravene any DMT policies
- it is not excessive in its use of resources

3. Use of services provided by third parties

Wherever possible, staff should only use services provided or endorsed by the DMT for conducting its business. The DMT recognises, however, that there are occasions when it is unable to meet the legitimate requirements of its members and that in these circumstances it may be permissible to use services provided by other third parties.

4. Unattended equipment

Computers and other equipment used to access DMT facilities must not be left unattended and unlocked if logged in. Staff must ensure that their computers are locked before being left unattended. Care should be taken to ensure that no restricted information is left on display on the computer when it is left unattended. Particular care should be taken to ensure the physical security of all equipment when in transit.

5. Unacceptable use

In addition to the above, the following are also considered to be unacceptable uses of DMT facilities:

- Any illegal activity or activity which breaches any DMT policy
- Any attempt to undermine the security of the DMT's facilities.
- Providing access to facilities or information to those who are not entitled to Access.
- Any irresponsible or reckless handling or unauthorised use of DMT's data (see the Information Handling Policy).
- Any use which brings the DMT into disrepute.
- Any use of DMT facilities to bully, harass, intimidate or otherwise cause alarm or distress to others.
- Sending unsolicited and unauthorised bulk email (spam) which is unrelated to the legitimate business of the DMT.
- Creating, storing or transmitting any material which infringes copyright.
- Creating, storing or transmitting defamatory or obscene material.
- Using software which is only licensed for limited purposes for any other purpose or otherwise breaching software licensing agreements.
- Failing to comply with a request from an authorised person to desist from any activity which has been deemed detrimental to the operation of the DMT's facilities.
- Failing to report any breach, or suspected breach of information security to the Chief Executive.
- Failing to comply with a request from an authorised person for you to change your password.

6. Penalties for misuse

Minor breaches of policy will be dealt with by the Chief Executive.

More serious breaches of policy (or repeated minor breaches) will be dealt with under the DMT's disciplinary procedures.

Where appropriate, breaches of the law will be reported to the police. Where the breach has occurred in a jurisdiction outside the UK, the breach may be reported to the relevant authorities within that jurisdiction.