MS-CAS ACCEPTABLE USE OF IT POLICY

This Acceptable Use Policy covers the security and use of all MS-CAS information and IT equipment. It also includes the use of email, internet, and mobile IT equipment.

This policy applies to all MS-CAS employees / volunteers (hereafter referred to as 'individuals').

This policy applies to all information, in whatever form, relating to MS-CAS activities.

Computer Access Control – Individual's Responsibility

Individuals must not:

- Allow anyone else to use their password on any MS-CAS IT system.
- Leave their user accounts logged in at an unattended and unlocked computer.
- Perform any unauthorised changes to MS-CAS IT systems or information.
- Attempt to access data that they are not authorised to use or access.
- Line managers must ensure that individuals are given clear direction on the extent and limits of their authority with regard to IT systems and data.

Internet

Individuals must not:

- Use the internet or email for the purposes of harassment or abuse.
- Use profanity, obscenities, or derogatory remarks in communications.
- Access, download, send or receive any data (including images), which MS-CAS considers offensive in any way, including sexually explicit, discriminatory, defamatory or libellous material.
- Use MS-CAS email / internet to gamble.
- Place any information on the Internet that relates to MS-CAS or alter any information about it, or express any opinion about MS-CAS unless they are specifically authorised to do this.
- Download copyrighted material such as music media (MP3) files, film and video files (not an exhaustive list) without appropriate approval.
- In any way infringe any copyright, database rights, trademarks or other intellectual property.
- Download any software from the internet without prior approval.

Working Off-site

- Information should be protected against loss or compromise when working remotely (for example at home or in public places).
- Particular care should be taken with the use of mobile devices such as laptops, mobile phones, smartphones and tablets. They must be protected at least by a password or a PIN and, where available, encryption.

Mobile Storage Devices

Mobile devices such as memory sticks, CDs, DVDs and removable hard drives must be used only in situations when network connectivity is unavailable or there is no other secure method of transferring data.

Software

Employees must use only software that is authorised by MS-CAS. Authorised software must be used in accordance with the software supplier's licensing agreements. All software used for MS-CAS must be approved by MS-CAS.

Monitoring

It is your responsibility to report suspected breaches of security policy without delay to Manager / Team Member / Trustees (depending whom you are).

All breaches of information security policies will be investigated.

Where investigations reveal misconduct, disciplinary action may follow in line with MS-CAS disciplinary procedures.

POLICY DATED: [16/11/2022*]*

REVIEW DATE : *2 years after date of policy*