CLEAN DESK POLICY

1. Policy Statement

1.1. The Society is mindful of the rights and obligations established by the **General Data Protection Regulation 2016** and the **Data Protection Act 2018** (hereinafter together "the Applicable Legislation") in relation to the management and processing of personal data. Equally, the Society is aware of the **ISO/IEC 27002 standard** (code of practice for information security management) and that it should be an integral part of the Society's approach to data management.

1.2. This Policy must be read in conjunction with other key Society's policies. In particular, colleagues should also be familiar with the **Data Protection Policy** and the **Acceptable Use of IT Facilities Policy**, both available on Colleagues Connect.

2. Purpose

2.1. This Policy has a dual purpose:

2.1.1. Ensure data protection compliance

To ensure that any personal data colleagues work with in their day-to-day job is treated in accordance with the legislation, and in the respect of the individuals whose personal data they process. These can be other colleagues, members, customers, contractors or any other third party whose personal data the Society processes.

The Policy aims to reduce the risk of data protection breaches in the workplace, and to increase colleagues' awareness about protecting and respecting people's personal data.

2.1.2. Improve working standards

To maintain good professional standards for colleagues and visitors and help promote respect for each other in our shared working environment.

3. Scope

3.1. The Policy applies equally to full-time and part-time colleagues on a substantive or fixed term contract, and to any associated persons who uses the Society's facilities such as agency staff, contractors and others employed under a contract of service.

3.2. The Policy applies to desk areas as well as other surrounding areas in colleagues' workspaces, ie. cabinets, meeting rooms and tables, photocopiers' areas etc.

3.3. All colleagues are responsible for making their affiliates or visitors aware of the guidelines in this Policy, and should check that hot desks have been cleared once their affiliates or visitors have left the Society's premises.

4. Policy Guidelines – Data Protection compliance

4.1. Colleagues are required to ensure that any personal data in hardcopy or electronic format is stored securely at the end of the working day, and when they are expected to be gone from their work area, or desk, for any length of time.

4.2. Computer workstations must be locked (CTRL + ALT + DELETE) when workspaces are unoccupied, or when the person using the computer/laptop is absent from the area.

4.3. Computer workstations must be shut down completely at the end of the working day.

4.4. File cabinets containing personal data must be kept closed and locked when not in use or when not attended. Keys used to access cabinets and drawers containing personal data must not be left at unattended desks.

4.5. Passwords must not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location. Equally, people's personal data (names/contact details etc.) must not be written on sticky notes and placed on computer screens.

4.6. All printers and fax machines should be cleared of papers containing personal data as soon as these are printed, to avoid being interjected or accidentally disposed of in ordinary bins.

4.7. Once no longer needed, documents containing personal data should only be shredded or placed in confidential disposal bins, where available. Colleagues should check with their line manager if unsure.

4.8. Whiteboards used during meetings or during the working day must be erased after use if they contain any type of personal data.

4.9. Portable computing devices such as laptops and tablets which aren't secured with a lockable cable at a desk should be stored in lockable cabinets or drawers when not in use.

4.10. Where their use is permitted by Society policy (see below), mass storage devices such as CDROM, DVD or USB drives containing personal data must be secured in locked drawers or cabinets when not in use.

4.11. By default, all USB ports on Society's computers and laptops are disabled. Colleagues who need to use USB ports on a regular basis to carry out their day-to-day job must contact the **Society's Data Protection Manager ("DPM")** for further guidance, and to be granted the necessary permissions.

5. Complying with the Policy

5.1. All colleagues are responsible for complying with the Policy. Line managers should monitor that these guidelines are enforced within their departments at all times.

5.2. Each business group's **Data Protection Champions ("DPCs")** should routinely verify compliance with this Policy through spot-checks and end-of-day checks in their business areas, and keep a record of any breaches of this Policy.

6. Policy Enforcement

6.1. In the event of a breach of this Policy, found either by a line manager or a DPC in the course of routine checks, the colleague responsible for the breach may be verbally warned that they are not adhering to the Policy, and reminded of the importance of handling personal data appropriately.

6.2. If several breaches reoccur and relate to the same colleague, a written warning may be given and, where the breach is of a particularly serious nature, a disciplinary action may be initiated.

7. More information?

7.1. For further information, or if you become concerned about potential risks in your business areas, or you have any other queries relating to data protection, please contact the relevant DPC in the first instance. A contact list of all the Society's DPCs can be found on Colleagues Connect.

Alternatively, colleagues may contact directly the Society's **Data Protection Manager[1] (DPM)** at data-protection@midcounties.coop)

8. Policy Guidelines – Improve Working Standards

8.1. In 2014, the following guidelines were agreed by the Society's Colleague Council, following a request from the Executive:

i. Two-tier desk trays (black) can be kept on desks and used to file current workload.
ii. Desk privacy screens must be kept clear of post-it notes, stickers, etc.
iii. One or two personal possessions, provided they are unobtrusive and of an appropriate size, can be kept on desks.
iv. Pens, pencils etc. must be stored in the pen tray within the desk's pedestal unit.
v. Mugs, cups and glasses should be removed from desks and cabinets' tops at the end of each day.
vi. As a general point, food should not be eaten at desks but should be consumed in the Orangery or other designated colleagues' areas. However, small snacks (ie. biscuits, fruit, etc.) and hot/cold drinks are acceptable.

8.2. It is important colleagues understand these guidelines are not intended to remove their individuality, but to maintain appropriate standards, and the necessary respect for each other, when colleagues, as well as visitors, share the same working spaces.

[1] Under the new data protection legislation, the Society had an obligation to formally appoint a Data Protection Officer (DPO) for its Healthcare, Phone Co-op and Energy businesses. The DPO's role is fulfilled by the Society's DPM.

8.3. All colleagues are responsible for complying with these guidelines. Line managers should monitor that these guidelines are enforced within their departments.

9. Changes to this Policy

9.1. This Policy will be reviewed when and as necessary and, in any case, at least on an annual basis by the Society's Data Protection Manager (DPM).