Active for all

Clear Desk and Screen Policy: Version 1 – 06/05/2021

1. **Clear desk**

The Company recognises that material left unattended (e.g. on a printer or in an unlocked cupboard) is more susceptible to damage, disclosure or theft, particularly outside of office hours.

Documents containing sensitive information according to the Company's Information Classification Scheme should be locked away when not required, especially when the office is empty. Printing should be removed from printers immediately and not left for others to pick up. Documents should be disposed of in the confidential waste bins or shredded according to the Company's Information Classification Scheme. No sensitive documents should be placed in the general waste.

Where possible, pedestals and/or shared cupboards should be locked when left unattended.

2. **Clear screen**

There is a risk that information could be viewed by unauthorised users if left on an unlocked, unattended computer screen. Screens can easily be locked when not in use by using Ctrl/Alt/Del and Enter or the Windows key and 'L' for Windows computers, or Control/Shift/Power for Macs. This should be done whenever a screen is left unattended.

For standard user accounts, screens will automatically lock after a period of 60 minutes when inactive. Administrator accounts will automatically lock after a period of 15 minutes when inactive.

3. Remote working

Care should be taken when working away from the office, including at home, to ensure that the same guidelines are followed. Always be aware of others being able to view Company material by 'shoulder surfing', especially when on public transport or in public locations such as cafes.

4. Removable media

All removable media devices including laptops and mobile phones containing SENSITIVE data should be stored within a secure room or cupboard when not in use.

Compliance

Failure to comply with this procedure could result in action in line with the Company's Disciplinary Procedure or Capability Procedure. Compliance checks will be undertaken by the Company's Information Governance functions. The results of compliance checks, their risk assessment and their remediation will be managed by the Information Security Board.