Process Id# :: **0005**
Process Name :: **NSSO Clean Desk Policy**
Date Last Updated :: **18/5/2019**

Description ::

To ensure the security and confidentiality of personal data and all other work related information, the National Shared Service Office (NSSO) has adopted a Clean Desk Policy for all desks, computers, devices and printers/photocopiers.

This policy ensures that all sensitive and confidential information, whether it be on paper, a storage device, or a hardware device, is properly locked away or disposed of when a workstation is not in use. This policy will minimise the risk of unauthorized access, loss of, and damage to personal data and any other information during and outside of normal business hours or when workstations are left unattended.

A Clean Desk Policy is an important security and privacy control and necessary for data protection compliance. This policy applies to all permanent, temporary and contracted staff working for or within the NSSO.

Policy

At all times, the following will apply:

- **All hardcopy and electronic data** must be kept secure.
    - Hardcopy items must be locked away in the relevant drawer or filing cabinet when desks are unoccupied and when the items are no longer in use.
    - Electronic files must be password protected at all times.
- **Computers** must be locked when the desk is unoccupied and completely shut down at the end of the work day.
- **Filing cabinets** must be kept closed and locked when not in use.
- **Laptops and mobile devices** must be secured when not in use, and removed from the desk and locked away in a drawer or filing cabinet.
- **Keys** for accessing drawers or filing cabinets should not be left unattended at a desk.
- **Passwords:** All passwords must be kept secure. No passwords may be written down.
- **Printers:** Any print jobs must be retrieved immediately. When printing, ensure that you are sending items to the correct printer.
- **Disposal of data:** All unnecessary paperwork left over at the end of the work day will be properly disposed of. Such data must be disposed of securely. Hardcopy items must be disposed of using confidential waste bags or shredding machines. Under no circumstances should such items be placed in regular waste paper bins.
- **Storage devices** such as USBs must be password protected and locked away when not in use.

Compliance

This policy will be officially monitored for compliance by line managers, the information governance team or Data and may include random and scheduled inspections.

Non-Conformance

All policies require the participation of staff and contractors to be successful. Any employee or contractor found to have violated this policy may be subject to disciplinary action.