Clear Desk Clear Screen

Contents

Policy Statement

Summary

This policy procedure summarizes the advice provided to all staff regarding clear desks and clear screens. By ensuring staff adhere to the policy the security and confidentiality of the Force's information assets are improved. The aims of this policy procedure are to:

- Demonstrate that the Force is taking corporate responsibility for the personal data in its care;
- Ensure staff keep data secure;
- Reduce the risks of unauthorised access to, loss of, or damage to data which has been left unattended; and
- Reduce the threat of identity theft or a security breach.

Scope

This policy/procedure applies to all Force personnel and includes partners, agency staff, sub-contractors and third part suppliers who may use Force premises and information technology infrastructure.

Only **current** personnel and vetted third party suppliers must be granted access to Force premises, equipment, data and infrastructure.

Clear Desk

Principles

- Where practicable, Individuals should lock information assets protectively marked as OFFICIAL or higher, in a suitable safe, cabinet, drawer or other storage furniture when not in use or would be leaving it unattended on a desk for a period of time, e.g. meeting or out at lunch etc.
- Where lockable storage is not available the room or office door should be locked if, and when, left unattended.
- The specifications for storage furniture depend on the classification of the information asset. For further information, please contact the Force Information Security Officer.
- Individuals should limit the use of sticky notes, memos or bits of paper, especially those containing personal information. They should be kept safe or shredded it when no longer needed.
- Drawings, images and photographs must not be displayed within reach of or in view of unauthorised personnel such as visitors, external contractors or cleaners. For example, photographs of nominal.
- Individuals should refrain from printing where possible, by reading information on screen. This reduces the amount of paper, containing important information, needed to be stored.
- New Konica Printers that are being installed across the Force require the individual to present their ID to retrieve their work.
- For old printers and fax machines, documents should be cleared from

printers and fax machines as soon as they are ready. This ensures that unauthorised personnel cannot pick up and read protectively marked documents left in printer trays.

NB It is worth noting that information assets left on desks are more likely to be damaged or destroyed in the event of a fire, flood or explosion.

Clear Screen

Principles

- Individuals are accountable for all computer activity, emails sent, and transactions entered using their user ID, whether or not they were present at the time.
- A password protected screen saver will activate after 15 minutes of inactivity but this is long enough for someone to compromise any available information or software systems.
- Individuals must always secure their computer:
  - **Lock** – when leaving unattended for any period of time. This can be done by pressing the windows key and the 'L' key at the same time. Or via the menu accessed by pressing 'Ctrl, Alt and Delete' at the same time. Individuals must confirm this action so another user cannot operate their machine via their user ID.
  - **Log off** – when finished working and another person is needing to use the computer. This can be done via the 'Start' menu. Or via the menu accessed by pressing 'Ctrl, Alt and Delete' at the same time. Individuals must confirm this action so another user cannot operate their machine via their user ID.
  - **Shutdown** – when finished working and no other person is needing to use it. This can be done by pressing the windows key and the 'L' key at the same time. Or via the menu accessed by pressing 'Ctrl, Alt and Delete' at the same time. Individuals must confirm this action so another user cannot operate their machine via their user ID.
- Computer screens should be angled away from the view of unauthorised persons. This could include external and internal windows and main doorways. This is particularly important when using a laptop in a public place.
- For individuals who are unable to angle their screen, privacy screens are available to prevent information being compromised. Contact should be made with the administration team or the Force Information Security Officer for more information.

General

Principles

- The Force Information Security Officer will conduct random unannounced audits and security audits and report non-compliance to the appropriate

management.
- Individuals who need to leave the office in an emergency, e.g. fire alarm or emergency call, must should lock their screen **only if it is safe to do so**, to prevent unauthorised access.

Responsibilities

All Officers and Staff

Responsibilities

Police officers and police staff are responsible for:
- Complying and demonstrating compliance with this policy. Failure to comply will be regarded as a disciplinary offence and be dealt with as such;
- Classifying information assets appropriately;
- Considering the security of the information assets they have access to and protecting them accordingly;
- Logging off or locking any Force computer, terminal, laptop or screen etc. when leaving it unattended;
- Keeping user IDs and passwords secure. Individuals must protect their passwords at all times, ensuring that they are of suitable strength and not divulged to anyone or recorded/written down under any circumstances, e.g. stored with a laptop;
- Protecting or supervising incoming and outgoing mail collection points so that letters cannot be lost or stolen; and
- At the end of a working day:
  - Closing down all software applications, logging off the Force computer, terminal, laptop or screen etc. and shutting them down; and
  - Clearing information assets protectively marked as OFFICIAL or higher from the desk and, where practicable, locking it in suitable safe, cabinet, drawer or other storage furniture or in a locked room or office.

Managers and Supervisors

Responsibilities

Managers and supervisors are responsible for:
- Ensuring their staff maintain a professional and tidy working environment; and
- Monitoring compliance on a regular basis.

Additional Information

Compliance

This policy complies with the following legislation, policy and guidance:

- HM Government's Security Policy Framework (SPF)
- HM Government's Security Classifications (GSC)
- National Policing Community Security Policy (CSP)
- Data Protection Act 2018 – GDPR
- Computer Misuse Act 1990
- Official Secrets Act 1989
- Electronic Communications Act 2000

Policy Database Administration

Item	Details
Document title:	Clear Desk Clear Screen
Owner:	Information Management
Author / Reviewer:	
Date of last review:	23/04/2019

The Equality and Human Rights Assessment for this policy is held on Force Registry which can be accessed via **this link**.

The table below details revision information relating to this document:	
Topic title	Date