



Clear Desk and Clear Screen Procedure

This procedure is part of North Yorkshire Police policy to which all Chief Constable personnel and the functions provided by the Police, Fire and Crime Commissioner are required to adhere.

Procedure Statement

The purpose of this procedure is to provide all North Yorkshire Police (NYP) officers and staff with guidelines and the procedures to follow, to prevent the compromise or theft of information and secure Force information systems when not in use.

Principle 7 of the Data Protection Act 2018 places a responsibility on organisations to ensure appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data against accidental loss or destruction of, or damage to, personal data.

The Official Secrets Act 1989 details the offences of unauthorised disclosure and failing to safeguard official information.

Police Digital Service's (previously The National Police Information Risk Management Team (NPIRMT) National Policing Community Security Policy (CSP) requires all members of the Police community to implement controls on the security marking of all types of information in their possession.

The Security Policy Framework (SPF) provides a baseline set of security requirements for safeguarding sensitive information.

Compliance with the HMG Security Policy Framework, HMG IA Standard No. 6 (Protecting Personal Data and Managing Information Risk (IS6)) and HMG Information Assurance Maturity Model (IAMM) are mandatory for all Forces and Agencies who are members of the NPIRMT CSP Community.

In order to provide a common standard within the Service and between partner agencies for the valuation of information assets, the Government Security Classification (GSC) was introduced in August 2016 following on from the Government Protective Marking Scheme (GPMS)

The Code of Practice for the Management of Police Information (MoPI) requires that all forces have policies and procedures in place to direct and control access to protectively marked documents. This further emphasises the importance of Protective Marking within the police service and the need for all forces to adopt policies and procedures to control access to police information and how that information is used.

Clear Desk and Clear Screen Procedure

Overarching Policies:

Force Information Security Policy

Procedures:

Protective Marking Procedure

Security Incident Reporting Procedure

Physical Security Procedure

Other Documents:

Information Systems Community Security Policy (CSP)

MoPI Guidance

Security Policy Framework (SPF)

Information Assurance Maturity Model (IAMM)

Process

This guidance has been updated to reflect the adoption of Government Security Classification (GSC) policy. The introduction of GSC means that a range of information of varying sensitivity is now classified as OFFICIAL. Some of the most sensitive OFFICIAL material will carry the security marking OFFICIAL-SENSITIVE, however a considerable number of OFFICIAL documents will not require any security marking at all. The lack of a visible security marking does not mean that a document does not contain sensitive information; it simply means that it does not meet the threshold for the OFFICIAL-SENSITIVE marking.

Throughout this procedure document, sensitive information is defined as “any information that may have some form of impact on the force or its functions if it were to be compromised”. Broadly speaking, this refers to any information that would previously have been categorised under GPMS as PROTECT or above. Further guidance on GSC can be found within the Protective Marking Procedure.

All NYP personnel processing information shall adopt both a clear desk and clear screen procedure.

Clear Desk

Papers and electronic data containing sensitive information shall be stored in suitable locked cabinets or drawers or secured behind a locked office door when not in use. This will reduce the risks of compromise, unauthorised access and disclosure, and loss of, and damage to, information whilst it is not being used or processed. Information left out on desks is more likely to be at risk through compromise or being damaged or destroyed in a disaster such as fire, flood, or explosion.

All information Protectively Marked SECRET or above must be secured in an appropriate (i.e. Security Equipment Assessment Panel (SEAP) approved) storage device. The same applies to some OFFICIAL-SENSITIVE material where originators have stipulated this as a handling condition. Further information can be obtained from the Information Security Officer and in the Physical Security Procedure.

Clear Screen

Clear Desk and Clear Screen Procedure

It is appreciated that staff will leave their computers, tablets, laptops or smartphones for breaks, meetings, etc., and the process of logging off a computer, tablet, laptop or smartphone and logging back on can be time consuming. However, in order to protect NYP systems and information, computers, tablets, laptops and smartphones must NOT be left logged on when unattended for prolonged periods of time.

Where staff must leave their computer, laptop, tablet, or smartphone unattended for short periods, they are to lock their hardware. A computer, laptop and tablet can be locked by pressing the Ctrl, Alt and Delete keys simultaneously (Ctrl, Alt and Insert on Wyse terminals) and/or clicking the lock button on-screen. To unlock the computer, tablet or laptop, staff should press the Ctrl, Alt and Delete keys simultaneously again and/or enter their PIN and/or Password at the on-screen prompts.

In the security of electronic data on smartphones, to protect any electronic data stored or displayed a user can lock the device by pressing the power button. Alternatively, the smartphone can be powered off by pressing and holding the power button. Smartphones should be securely protected and stored when not in use.

Under no circumstances shall a member of staff leave their computer, tablet, laptop, or smartphone logged-on and unlocked when unattended.

Where a computer, tablet or laptop is shared by numerous officers, such as computers located in briefing rooms, users must log-off when leaving the hardware unattended rather than locking the hardware.

To enhance security, an automatic screen lock timeout is applied to NYP's computers, tablets, laptops and smartphones, however, it is still the personal responsibility of the user to carry out the steps above to lock the screen when leaving their desk or leaving the hardware unattended. To unlock the screen, follow the above process.

Other Devices

Documents marked with the security classification of OFFICIAL SENSITIVE received on Fax machines should be removed immediately and especially when vacating the office. Fax machines used for OFFICIAL SENSITIVE (or above) material must be located in rooms that can be secured.

If a photocopier/printer is fitted with a key code, this code should be activated, not only to control access to the copier/printer, but it will also be an audit for budget controls. Copiers/printers that are not key code protected should, if possible, be located in areas that can be secured.

Protectively Marked information marked as OFFICIAL- SENSITIVE and above, when printed, must be cleared from printers immediately and stored appropriately when not in use.

Summary

The originators (creators/authors) and users of all sensitive information are responsible for ensuring that access to this information, either internal or external, does not jeopardise any part of Force information, systems or data held on those systems. In particular, they must NOT:

- allow another users access to their password;

- allow information to be viewed by non-authorised personnel whilst displayed on screens or on hardcopy printouts left in printers, faxes or unattended desks;
- try to circumvent the security features or procedures of any NYP system.

The originators or users of all information are also responsible for following the appropriate reporting procedures, in a timely fashion, in the event of discovering or suspecting that a security incident has occurred. More information can be found in the Security Incident Reporting Procedure.

Any user that breaches NYP security policies and procedures may be investigated, which may in turn lead to disciplinary action and/or prosecution.

Responsibilities

Operational Officers/Police Staff

While there is no requirement to secure non-sensitive information, staff must:

consider if any part of the document sensitive in nature but fails to meet the criteria for the OFFICIAL-SENSITIVE protective marking;

- ensure all sensitive material is securely stored when not in use;
- lock screens when not in use;
- remove sensitive material from faxes, printers etc.

First Line Supervision

In addition to the responsibilities above, Line managers are responsible for ensuring staff comply with the Clear Desk/Clear Screen Procedure. Line managers are also responsible for ensuring the appropriate storage equipment is available to enable staff to comply with this procedure.

Safer Neighbourhood Commanders and Heads of Functions

In addition to the responsibilities above, Safer Neighbourhood Commanders and Heads of Functions must ensure staff and officers are aware of, and comply with, the Force Clear Desk/Clear Screen Procedure and its inclusion within any Information Sharing Agreements.

Safer Neighbourhood Commanders and Heads of Functions are responsible for submitting written justification via email to alter the Force wide automatic screen lock timeout for their teams or units.

Authorisation to alter the Force wide automatic screen lock timeout must be obtained from the Head of Information Management who will seek input from the Information Security Officer. Once authorisation has been obtained, the Head of Information Management will liaise with ICT to implement any agreed changes.

Command Team

Overall responsibility for the security of all information assets.

Definition of Special Terms

Clear Desk and Clear Screen Procedure

GPMS	-	Government Protective Marking Scheme
GSC	-	Government Security Classifications
MoPI	-	Management of Police Information
CSP	-	PDS National Policing Community Security Policy
SPF	-	Security Policy Framework
IAMM	-	Information Assurance Maturity Model