Handling of Protectively Marked Material

A Guide for Police Personnel (October 2001)

National Police Training

PITO

ACPO

ACPOS

Introduction

In moving towards more integrated working within the Criminal Justice System it is becoming increasingly important to ensure official documents and other data sources (both paper and electronic), to be known as information assets, are adequately protected and managed.

The ACPO/ACPOS Information Systems Community Security Policy requires community members to implement controls on the security marking of all forms of data in their possession.

In order to provide a common standard within the Service and between partner agencies, for valuation of information assets, the Chief Constables' Council ratified the adoption of the 'Protective Marking Scheme' in January 2001.

Personnel need to be aware that it is important that protective security practices:

- implement the 'need to know' principle
- are workable and user-friendly
- deal with all the prevailing threats
- are effectively co-ordinated by the personnel who use them
- are just, open and reasonable, where they may impinge on the lives of staff.

When selecting the appropriate marking, personnel should also consider:

- how damaging the consequences would be if material was lost, stolen, disclosed or destroyed
- correct marking is applied (over or under classification damages the credibility of the system)
- a compilation of many items marked at the same level may require the whole to be marked at a higher level
- the scheme should not be used to protect against sensitivities likely to arise due to inefficiency or administrative error
- regular reviews of the material may be necessary in order to downgrade or destroy any such material.

There are four levels of Protective Marking that can be applied to sensitive assets, depending on the degree of sensitivity involved:

1. RESTRICTED*
2. CONFIDENTIAL*
3. SECRET*
4. TOP SECRET*.

The majority of information held within the Police Service contains personal or sensitive data and therefore requires a level of Protective Marking.

(Information that has been obtained from sources, which are publicly available, will not require a protective mark.)

This guide predominantly deals with assets that are marked at either RESTRICTED or CONFIDENTIAL, as they comprise the vast majority of 'sensitive' information assets held within the Police Service.

If you are confronted by SECRET or TOP-SECRET assets, contact your own force ISO (Information Security Officer) for advice on the correct method of handling them.

**NB – When used as a Protective Marking – the words RESTRICTED / CONFIDENTIAL / SECRET and TOP SECRET, will be displayed in capitals to differentiate them from ordinary useage within documents.*

The same rule applies when attaching a descriptor (see later) all DESCRIPTORS will be written in capital letters.

Impact Criteria - Protective Markings

Restricted

Would accidental or deliberate compromise of assets marked **RESTRICTED** be likely to:

- **cause substantial distress to individuals;**
- make it more difficult to maintain the operational effectiveness or security of the UK or allied forces;
- **prejudice the investigation or facilitate the commission of crime;**
- impede the effective development or operation of government policy;
- **breach proper undertakings to maintain the confidence of material provided by third parties**;
- **breach statutory restrictions on disclosure of material (does not include the Data Protection Act 1998, where non-sensitive information is involved);**
- **disadvantage** government or **the police service in commercial or policy negotiations with others**;
- **undermine the proper management of the public sector and its operations**.

Confidential

Would accidental or deliberate compromise of assets marked **CONFIDENTIAL** be likely to:

- materially damage diplomatic relations, that is, cause formal protest or other sanctions;
- **prejudice individual security or liberty;**
- **cause damage to** the operational effectiveness or security of UK or allied forces or **the effectiveness of valuable security or intelligence operations;**
- work substantially against national finances or economic and commercial interests;
- substantially undermine the financial viability of major organisations;
- **impede the investigation or facilitate the commission of serious crime**;
- seriously impede the government policies;
- shut down or otherwise substantially disrupt significant national operations.

Secret

Would accidental or deliberate compromise of assets marked **SECRET** be likely to:

- raise international tension;
- seriously damage relations with friendly governments;
- **threaten life directly, or seriously prejudice public order, or individual security or liberty**;
- **cause serious damage to** the operational effectiveness or security of UK or allied forces or **the continuing effectiveness of highly valuable security or intelligence operations;**
- cause substantial material damage to national finances or economic and commercial interests**.**

Top Secret

Would accidental or deliberate compromise of assets marked **TOP SECRET** be likely to:

- **threaten directly the internal stability of the UK** or friendly countries;
- **lead directly to widespread loss of life;**
- **cause exceptionally grave damage** to the effectiveness or security of UK or allied forces or **to the continuing effectiveness of extremely valuable security or intelligence operations**;
- cause exceptionally grave damage to relations with friendly governments;
- cause severe long term damage to the UK economy**.**

‘Protective Marking’ is the method by which the ***originator*** of an asset (that is all material assets, ie papers, drawings, images, disks and all forms of electronic data records), indicates to others, the levels of protection required when handling the asset in question, in terms of its sensitivity, security, storage, movement both within and outside the originator’s own department or force and its ultimate method of disposal.

When a protective marking is applied to a sensitive asset it is indicating its value in terms of the damage that is likely to result from that information being compromised, eg when applying a protective marking of CONFIDENTIAL in relation to serious crime, it is because the compromise of that information would be likely to impede the investigation or facilitate the commission of serious crime, not simply refer to any material concerning a serious crime.

The sections on this page detail the criteria for each level of Protective Marking and are derived from the Protective Marking Scheme and sections considered to apply to routine policing are **emboldened**.

Handling rules regarding protectively marked material

Restricted	Your Action	Confidential
Top and bottom of every page.	Marking	Top and bottom of every page.
Protected by one barrier, eg a locked container within a secure building.	Storage of papers	Protected by **two** barriers eg a locked container in a locked room, within a secure building.
Use secure waste sacks. **Keep secure when left unattended.**	Disposal of papers	Downgrade by tearing into small pieces and place in secure waste sacks, or use a cross cut shredder. **Keep secure when left unattended.**
Securely destroy. Floppy disk - dismantle and cut disk into quarters (at least), dispose with normal waste. CD Roms - destroy completely - disintegrate, pulverise, melt or shred.	Disposal of magnetic media	Securely destroy. Floppy disk - dismantle and cut disk into quarters (at least), dispose with normal waste. CD Roms - destroy completely - disintegrate, pulverise, melt or shred.
In a sealed envelope with protective marking shown. A transit envelope **may** be used if sealed with a security label.	Movement within force via internal dispatch	In a new sealed envelope with protective marking shown. Transit envelopes **must not** be used.
By post or courier, in a sealed envelope. **Do not show** protective marking on the envelope.	Movement between forces/partner agencies	By post or courier. Double enveloped and both fully addressed. Protective marking shown on inner envelope only. Return address on **outer** envelope.
May be used.	Force internal and public telephone network	Only if operationally urgent. Use guarded speech and keep conversation brief.
Digital cellphones may be used. Only use analogue cellphones if operationally urgent, use guarded speech and keep conversation brief.	Mobile telephone (voice and text)	Digital cellphones may be used but **only** if operationally urgent. Use guarded speech and keep conversation brief.
Not to be used.	WAP telephones	Not to be used.
Use of police radio network is an essential tool for policing. Criminal elements and other untrustworthy persons continually monitor the network. Care should be taken when disclosing information of a sensitive or personal nature and if not operationally urgent another means of communication must be sought.	Police Radios pre 'AIRWAVE'	*Only if operationally urgent. Use guarded speech and keep conversation brief.
Not to be used.	Pager systems	Not to be used.
May be used.	Force Data Network/Criminal Justice Extranet	May be used in conjunction with CESG Enhanced Grade Encryption.
Government approved encryption required.	Internet	Not to be used.
Check recipient is on hand to receive. Send cover sheet first and wait for confirmation before sending.	Fax	Use secure fax machine only.

*If there is a requirement to use any of the above methods of communication at a higher level than recognised safe to do so, the operational urgency and the need for transmission must be weighed against the risk of a security breach, for which the force may be held accountable. If it is decided that such transmissions are essential, they should be kept short and guarded speech used. The use of some form of prearranged codes should be considered to avoid identifying officers, informants or locations.

Requirements and restrictions on the handling/disposal etc of SECRET and TOP SECRET material are not included in this aide-memoire. Should you find yourself confronted with or required to deal with such material, seek advice or assistance from your force Information Security Officer, who will be able to advise you accordingly.

Descriptors

When you originate material requiring a Protective Marking, you ***may,*** if necessary, add a DESCRIPTOR where it ***helps indicate to others*** the nature of the sensitivity and the groups of people who need access.

No specific DESCRIPTORS are mandated, but it is recommended that in order to adopt a common standard the following are considered:

APPOINTMENTS
concerning actual or potential appointments that have not yet been announced

COMMERCIAL
relating to a commercial establishments processes or affairs

CONTRACTS
concerning tenders under consideration and the terms of any tenders

CRIME
concerning crime

INTEL
concerning intelligence

HONOURS
unannounced recognition for exceptional achievement

CHIS
(Covert Human Intelligence Source) regarding informants and their handling. Any informant related information should be protectively marked CONFIDENTIAL as a baseline, with the appropriate handling procedures. Information which identifies an informant should be marked SECRET

INVESTIGATIONS
concerning investigations into disciplinary or criminal matters, involving members of the police service

MANAGEMENT
policy and planning affecting the interest of groups of staff

MEDICAL
medical reports, records and material relating to staff

PERSONAL
material intended for the person to whom it may be addressed

POLICY
proposals for new or changed force policy, prior to publication

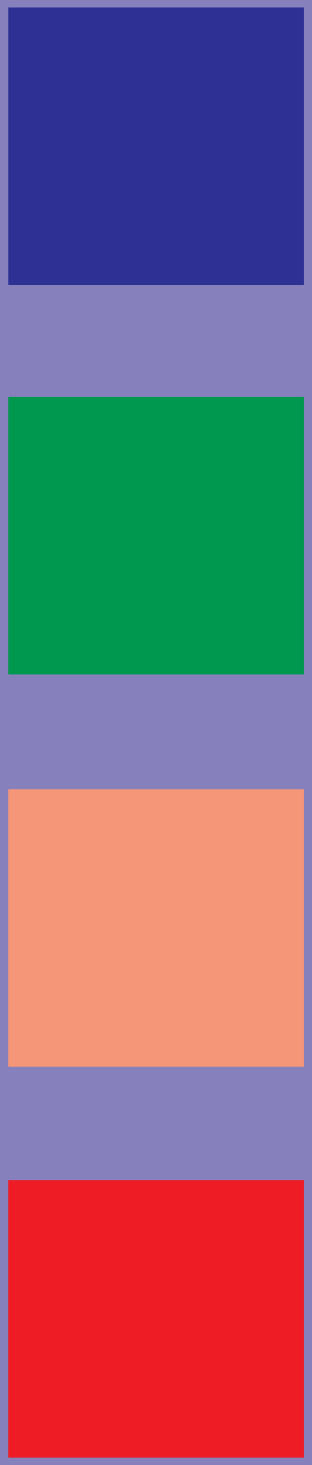
PRIVATE
for information collected through electronic government services provided to the public and agencies and relating to the individual or agencies

STAFF
concerning references to named or identifiable staff or personal confidences entrusted by staff to management

VISITS
concerning details of visits by, for example, royalty, ministers and other dignitaries.

With the exception of PERSONAL or PRIVATE, which may be used by themselves, the above descriptors may only be used in conjunction with a protective marking.

Special handling instructions may also take the form of caveats, nicknames and code words or exceptionally other handling instructions eg DESCRIPTOR may take the form of an operation name – such as - "OPERATION RAINBOW"– EYES ONLY.



This leaflet is designed to inform staff of procedures and help them determine and indicate to others, the levels of protection required when handling official documents.

The term document refers to all material assets, ie papers, drawings, images, disks and all forms of electronic data records.

This leaflet is designed as an **aid** only. Further and more comprehensive guidance can be found in the Manual of Protective Security or from your own force ***Information Security Officer***.

Your ISO Contact details are:

National Police Training

Enquiries Telephone 01603 621000

(Compiled with grateful acknowledgement to the Crown Prosecution Services' "Handling of Protectively Marked Material" Guide published June 2001 and 'Protective Marking – A guide to understanding and using the Protective Marking Scheme from the perspective of the Police Service', by Paul Harding, Hampshire Constabulary, July 2001.)

File ref: NPT/TSG/TrainDes/119/ms