PS 171 Government Protective Marking Scheme (GPMS) Policy

October 2013
Version 1.0

Statement of legislative compliance

This document has been drafted to comply with the general and specific duties in the Equality Act 2010; Data Protection Act; Freedom of Information Act; European Convention of Human Rights; Employment Act 2002; Employment Relations Act 1999, and other legislation relevant to policing.

Table of Contents

Aims and objectives of the policy

1.1 To ensure our legal use of information/intelligence is balanced with the needs of information/intelligence security and to ensure that the force complies with the Association of Chief Police Officers (ACPO) Council decision to adopt the Government Protected Marking Scheme and reflects relevant considerations regarding the Code and Guidance of the Management of Police Information.

1.2 The protective-marking scheme is a method for creating a common standard within the police service for the valuation and protection of the information assets available within the service.

1.3 The purpose of this document is to implement the necessary controls contained within the Security Policy Framework in the context of the business requirements of Nottinghamshire Police.

1.4 The policy applies to the protection of all information (manual or electronic). By protectively marking our information assets the sensitivity of the material is assessed by determining the likely consequences of that material being compromised.

1.5 This policy will enable the Force to:

- apply appropriate protective measures to our material according to the likely consequences of its compromise;

- have a common understanding with government departments and other police forces about the measures required to protect shared material in matters such as organised crime, drugs trafficking and intelligence;

• have a common understanding with other agencies about measures needed to protect any material that we pass to them; and

- have a common understanding with contractors and suppliers about measures needed to protect any material that we pass to them in compliance with any relevant protocols.

1.6 The main aims and objectives are:

- Applicable to all authorised users of Nottinghamshire Police Information and is therefore applicable to all staff, whether permanent or temporary and to any third party contractors or partners who have access to such information.
- **Confidentiality** – ensuring that information/intelligence is accessible only to those authorised to have access and protecting assets against unauthorised disclosure.
- **Integrity** – safeguarding the accuracy and completeness of information and processing methods, and protecting assets from unauthorised or accidental modification.
- **Availability** – ensuring that authorised users have access to information and associated assets when required to pursue Nottinghamshire Police objectives.

This policy is part of a suite of guidance that links to the Force Information Security Policy. As such users need to take cognisance of the national Code and Guidance related to the Management of Police Information.

Policy statement

2.0 The origins/background information:

In January 2001 the Association of Chief Police Officers (ACPO) Council agreed that implementation of the Government Protective Marking Scheme (GPMS) should be adopted throughout all police forces.

The main benefits of implementing the scheme throughout the police service are the increased opportunities for partnership working, improved handling of sensitive information and the improved evaluation of the security measures required to protect information.

2.1 Motivators/Driving Forces:

Information and intelligence is accepted as the lifeblood of effective policing and must receive adequate protection. To provide a recognised system for this purpose ACPO has accepted the Government Protective Marking Scheme (GPMS) for implementation across the police service.

GPMS provides a consistent standard for the marking of sensitive assets. It therefore is an enabler regarding the correct collection, review, evaluation, sharing or retaining of such information/intelligence.

2.2 General Principles of the Policy:

The majority of information held within the police force is sensitive and requires a protective marking value. The marking, an information asset requires, will be ascertained by identifying what would happen if the information was to be compromised.

Consideration has to be given to the impact upon an individual, the Force, major organisations and national security.

The effectiveness of this system is closely linked to the “Need to Know” approach to information management and to the Force Vetting Policy. Fundamental to the principles of protective marking is the fact that “Need to Know” has dual interpretation ~ restricting information to those who have a need for such information and ensuring that those who do require that information are not prevented from receiving it.

Protective Marking is one of a series of controls Nottinghamshire Police will utilise in order to protect its information assets. The policy and procedures are derived from the Security Policy Framework.

This policy provides the appropriate controls for the marking, handling, movement, storage and disposal of sensitive material.

2.3 Need to Know:

One of the major principles of the Protective Marking scheme is the “Need to Know” principle. This principle states that only individuals with a legitimate reason for obtaining information are able to do so. For example, only those individuals directly involved with an investigation into serious crime have the right to access information held relating to that crime. Other members of the same Force / Station have no legitimate need to view the information. “Need to Know” also means there is a requirement to inform those with an operational or business need to access the information.

In order for Protective Marking to be effectively implemented, it is important that staff understand and view the principles contained within the “Need to Know” doctrine as an enabling mechanism.

The purpose of this principle is to allow members of staff to provide and receive information that is relevant and helpful to the Force’s specific business needs and those of the proposed recipient of the information.

It introduces a simple decision making process when members of staff are in a position to disclose information, by asking themselves whether the recipient needs to know, for their business purposes:

• All of the information

• Some of the information, or

• Any of the information.

The application of this principle will enable members of staff to supply and receive information in pursuance of Police business. This ensures all the disclosures of information

either within the Force, or externally to other partnership and law enforcement agencies, will meet the requirements set by Legislation and Force Policy

2.4 Protective Marking Criteria

All information assets will either not be protectively marked (and thus unprotected) or utilise one of the four classifications of:

- PROTECT, Impact levels 1 and 2
- RESTRICTED, Impact level 3
- CONFIDENTIAL, Impact level 4
- SECRET, Impact level 5
- TOP SECRET, Impact level 6

In addition where an information asset requires special handling instructions an approved descriptor may be attached to that asset, for example: RESTRICTED-MEDICAL; CONFIDENTIAL-INTEL; CONFIDENTIAL-OPERATION LITOTES; SECRET-CHIS. (See below).

Information that either has been obtained from the public domain, or due to its content may be disclosed to the public domain (e.g. contents do not fit into the above four categories), will be identified as “Not Protectively Marked”

The following sections define the above levels. The areas particularly relevant to police work are outlined in bold:

2.5 PROTECT - The compromise of assets marked PROTECT would be likely to:

Impact level 1

No impact on life and safety

- Minor disruption to emergency service activities that requires reprioritisation at local (station) level to meet expected levels of service
- No impact on crime fighting
- No impact on judicial proceedings

Impact level 2

- Inconvenience or cause discomfort to an individual
- Minor disruption to emergency service activities that requires reprioritisation at area / divisional level to meet expected levels of service
- Minor failure in local Magistrates Courts

PROTECT is not a national security protective marking and the policy relating to the use of RESTRICTED remains unchanged.

PROTECT is not to be used for operational issues.

PROTECT must be accompanied by a Descriptor, (e.g. PROTECT – STAFF).

AIMS	BASELINE MEASURES	ACCESS
To promote discretion in order to avoid unauthorised access	Make accidental compromise or damage unlikely during the storage, handling, use, processing, transmission or transport.	Need to Know principle + Basic Check (BC). May require a Counter Terrorist Check (CTC).
	Avoid deliberate compromise or opportunistic attack.	
	Dispose or destroy in a manner to make reconstruction unlikely.	

2.6 RESTRICTED - The compromise of assets marked RESTRICTED would be likely to:

- Adversely affect diplomatic relations
- 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
- Breach proper undertakings to maintain the confidence of information provided by third parties
- Impede the effective development or operation of government policies
- Breach statutory restrictions on disclosure of information (does not include the Data Protection Act 1998, where non-sensitive personal information is involved)
- Disadvantage government in commercial or policy negotiations with others
- Undermine the proper management of the public sector and its operations

AIMS	BASELINE MEASURES	ACCESS
To promote discretion in order to avoid unauthorised access	Make accidental compromise or damage unlikely during the storage, handling, use, processing, transmission or transport.	Need to Know principle + Basic Check (BC). May require a Counter Terrorist Check (CTC).
	Avoid deliberate	

	compromise or opportunistic attack.	
	Dispose or destroy in a manner to make reconstruction unlikely.	

2.7 CONFIDENTIAL – The compromise of assets marked CONFIDENTIAL would 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 (Serious crime as defined by the Regulation of Investigatory Powers Act 2000 see Sect. 81(3)).

- Seriously impede the development or operation of major government policies.

- Shut down or otherwise substantially disrupt significant national operations.

AIMS	BASELINE MEASURES	ACCESS
	Make accidental compromise or damage unlikely during the storage, handling, use, processing, transmission or transport.	BASIC CHECK (Compulsory)
	Control knowledge of planned movement of physical assets.	In some cases a Counter Terrorist Check (CTC) or certain elements of a Security Check (SC) may be required
To attempt to help in the identification of persons responsible for the compromise of confidential material	Offer a degree of resistance to deliberate compromise.	
	Detect actual or attempted compromise and help in the identification of the individual(s) responsible.	
	Dispose or destroy in a manner to make reconstruction unlikely.	

2.8 SECRET - The compromise of assets marked SECRET would 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.

AIMS	**BASELINE MEASURES**	**ACCESS**
Ensure there is no unauthorised access to SECRET material Any attempt will be detected and those responsible identified.	Make accidental compromise, or damage, highly unlikely during the storage, handling, processing, transmission or transport.	Users must have undergone a Security Check (SC) In some cases where limited access is required to SECRET assets a basic check may be sufficient.
	Limit knowledge of planned movement of physical assets.	
	Offer a degree of resistance to deliberate compromise by a professional or violent attack.	
	Offer a degree of resistance to deliberate compromise and help in the identification of the individual(s) responsible.	
	Dispose or destroy in a manner to make retrieval or reconstruction highly unlikely and prevent identification of constituent parts.	

2.9 TOP SECRET - The compromise of assets marked TOP SECRET would 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.

AIMS	BASELINE MEASURES	ACCESS
Ensure there is no unauthorised access to TOP SECRET material	Prevent accidental compromise, or damage, during the storage, handling, processing, transmission or transport.	Users must have undergone Developed Vetting (DV)
	Strictly Limit knowledge of planned movement of physical assets to those with a 'Need to Know'.	
Any attempt will be detected and those responsible identified	Offer a degree of resistance to liberate compromise by a sustained and sophisticated or violent attack.	In some cases where limited access is required to TOP SECRET assets a Security Check (SC) may be sufficient
	Detect actual or attempted compromise and make it likely that individual(s) responsible will be identified.	
	Dispose or destroy in a manner to make retrieval or reconstruction highly unlikely and prevent identification of constituent parts.	

2.10 DESCRIPTORS

In addition to the use of a protective-marking classification it is also possible to further label assets with a descriptor. A descriptor is applied if the asset may require specific handling considerations. This not only helps in the handling of the asset BUT also enhances the users' ability to assess the necessity of applying the "Need to Know" principle.

A descriptor is not essential but may be added to help indicate the nature of the sensitivity and the groups of people who need access. The following descriptors, which are not exhaustive, may be used.

Whilst the Security Policy Framework does not mandate specific descriptors, there are certain descriptors used throughout the public sector, which should be considered for the purpose of consistency. The following are commonly used descriptors, which should be considered where appropriate.

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

CHIS (Covert Human Intelligence Source) - regarding informants and their handling. Any informant related information shall be treated at as baseline CONFIDENTIAL with the appropriate handling procedures. Information that identifies an informant may require marking at SECRET

COMMERCIAL - relating to a commercial establishment's processes or affairs;

CONTRACTS - concerning tenders under consideration;

CRIME - concerning crime;

HONOURS - recognition given for exceptional achievements.,

INTEL - criminal intelligence.,

INVESTIGATIONS - concerning investigations into disciplinary or criminal matters;

MANAGEMENT -policy and planning affecting the interests of groups of staff;

MEDICAL - medical reports and records and material relating to staff;

OPERATION 'NAME' – to restrict material to those involved in the operation

PERSONAL - material intended for the person to whom it is addressed-;

POLICY - proposals for new or changed government or Force policy before publication;

PRIVATE – for information collected through electronic government services or provided to the public and agencies and relating to the individual or agencies (see 6.3 below).

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 and ministers of state.

With the exception of PERSONAL and PRIVATE, which may be used by themselves, the above descriptors may only be used in conjunction with a Protective Marking. e.g. RESTRICTED – MEDICAL. This does not relate to the title of any file or folder.

Information sent to either an individual member of the public, or an organisation that does not subscribe to the Security Policy Framework will be marked with a descriptor of PRIVATE. In order to minimise disruption to the Force, information sent to Partnership Agencies will retain the relevant Protective Marking. Guidance will be provided to as required to Partnership Agencies as to the handling requirements of such information.

2.11 BASELINE MEASURES

Information assets marked as SECRET and TOP SECRET will routinely only be stored by the Force Special Branch.

No information or data marked above RESTRICTED should be stored or processed on the Force Network.

The key to successful use of Protective Marking is consistent marking, which requires a common-sense approach by the originator of the material. If material is originated which requires a PROTECT, RESTRICTED or CONFIDENTIAL marking, it must be marked at the time of origin. Some Nottinghamshire Police systems are not GPMS compliant and do not contain a GPMS marking on any printed material. It is the responsibility of any persons printing documents to ensure that the correct GPMS marking is written clearly or stamped on the document.

The protective marking must be conspicuous so that the value of the material is clearly conveyed to those who need to know to ensure all those who may handle it are aware of the level of protection required. The marking will be at the top and bottom of every page (within the ‘Header’ and ‘Footer’) in capitals and in black font.
The protective marking of any material must not be downgraded without referring back to the originator.

Increasing the protective marking of a document or a file containing a number of documents will be at the discretion of the individual handling it, subject to the principles in this policy. This will normally be achieved by placing it within a folder indicating the higher level of security, previous routing will be retained with the folder.

Care should be taken when handling information from agencies that do not mark their information assets. It is recommended that any information containing details of either a sensitive and/or personal nature should be treated as RESTRICTED. This includes information bearing the descriptor of PRIVATE. Old material bearing any form of IN CONFIDENCE marking should be treated as if it were at least RESTRICTED.

Protectively marked material must only be produced, handled and reproduced by persons with authorised access to it. The “Need To Know” principle must be applied, limiting material to those with a genuine “Need to Know” in order to discharge their duties. In particular, careful thought should be given to limiting the production of copies.

CONFIDENTIAL material should be regularly reviewed to consider the issue of protective marking with a view to downgrading or disposal in accordance with the Force policy on the retention of information.

Any protectively marked document should be stored within the appropriate secure environment when it is not being worked upon.

2.12 DISCLOSURE OF PROTECTIVELY MARKED MATERIAL

Protective Marking will assist in the protection of sensitive material, but the absence of a protective marking does not necessarily mean that the material may be made freely available. Conversely, the presence of a protective marking does not mean the material should not be disclosed in appropriate circumstances (for example, release of personal data to data subjects under the provisions of the Data Protection Act or to other bodies under the provisions of the Crime and Disorder Act).
Some Nottinghamshire Police systems are not GPMS compliant and do not contain a GPMS marking on any printed material. It is the responsibility of any persons disclosing or sharing information to ensure that the correct GPMS marking is written clearly or stamped on any such material.

Protective Marking does not mean that the material can be withheld under Freedom of Information legislation unless an exemption applies. Any disclosure of information must be in accordance with current Force Policy.

2.13 IMPLEMENTATION

The implementation of Protective Marking requires the Force to undertake a cultural change in its understanding and methods for the marking, handling, movement, storage and disposal of ‘sensitive’ material.

A full ‘clear desk’ policy must be the aspiration of this policy. This will have to be an ongoing consideration as office accommodation is updated and budget considerations need to be coordinated to meet the above overall timescales.
Any further detailed advice on Protective Marking and in relation to the Security Policy Framework may be sought from the Force Information Security Manager.

2.14 CLEAR DESK POLICY

Whilst it is impossible to offer guidance on every possible example related to this issue, a risk assessment process should apply which is closely related to the GPMS marking of the document or information/intelligence. In practical terms this means that the more sensitive the information/intelligence is then the greater care that must be taken to ensure that unauthorised persons do not have access to it e.g. by being able to easily read it in passing on paper or on a computer screen.

It is the responsibility of all business managers to ensure that their staff understand the meaning of ‘clear desk’ in context to their particular place of work and that they regularly ‘police’ their clear desk requirements to make sure staff comply with them.

The following should be seen as minimum standards to be expected:

All authorised users are expected to take a responsible attitude to the protection of information/intelligence during temporary periods away from their place of work. A risk

assessment process should be undertaken by the individual, which takes into account, at least, the time away from the intelligence/information, any possibility of unauthorised access to the information/intelligence whilst away from it, the nature of the GPMS marking on it and the level of risk the location presents in respect of unauthorised disclosure and/or misuse.

For more permanent periods away from the intelligence/information e.g.

- At the end of each working day and/or
- When the information/intelligence is no longer in use and/or
- When the work area is to be vacated such as for rest breaks

Particular care must always be taken to protect the intelligence/information from ‘third party’ (e.g. cleaners, maintenance engineers, members of the public, misc. contractors etc.) visitors to places of work who are not authorised to read/view police information/intelligence. Managers/supervisors and users should be aware who has access to keys to offices particularly during hours when places of work may not have authorised staff working in them and should ensure that relevant information cannot be viewed by any unauthorised staff.

Related documents and Appendices

ACPO GPMS LEAFLET DATED APRIL 2007

Administration

Version Control	
Section changed	**Details of change**

Monitoring and review	
Measure	**Date/period and process of review**

Registered Owner	
Owner	**Author**
Head of Professional Standards	Information Security Manager