Protective Marking Procedure

This procedure is part of North Yorkshire Police policy to which all Chief Constable personnel and the functions provided by the Deputy Mayor for Policing as part of the York & North Yorkshire Combined Authority are required to adhere.

Procedure Statement
In order to provide a common standard within the Police Service and between partner agencies for the valuation of information assets, the National Chief Constables' Council (NPCC) ratified the adoption of the Government Security Classification (GSC) in January 2016 and the North Yorkshire Police (NYP) Protective Marking Procedure was amended in September 2016.

Those handling police information have a responsibility to value and safeguard all information they send or receive. Where necessary, the appropriate classification and measures should be clearly identified in order to enable sharing and to protect from loss, damage or unauthorised and inappropriate access to the information. Classification ensures that police information is handled appropriately in order to protect individual rights in accordance with the law and with respect for the wider public interest.

All 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 prevailing threats;
- are effectively coordinated by the personnel who use them;
- are just, open and reasonable, where they may impinge on the lives of staff.

Overarching Policies:
Information Security Policy
Records Management Policy

Procedures:
Internet and E-mail Procedure
Clear Desk/Clear Screen Procedure
Working with Portable Media and Documents Procedure
Information Sharing Procedure
Freedom of Information (FOI) Procedure
Data Protection Procedure

Other Documents:
Appendix A – Information Asset Control Measures for 'OFFICIAL'
HMG Security Policy Framework
College of Policing APP (Authorised Professional Practice) for MoPI (Management of Police Information)
Secure Communications Guidance

Process

Overview
A Protective Marking gives a value to an information asset and an indication to those handling it as to how that document should be protected. It does this by determining the amount of damage that would be caused if the document was compromised (i.e., disclosed or destroyed), either accidentally or deliberately to unauthorised people. It provides an assurance that assets of broadly equivalent value are given the required and consistent level of protection. This relates to any assets wherever it is hosted, be it on premises or in an approved cloud environment.

An information asset is normally a document but can also be other forms of information. Some examples of information assets are:

- Briefing papers
- Reports
- Computer records
- Staff and medical records
- Intelligence
- Crime records
- Finance records
- E-mail

Under GSC, there are three different classifications that can be applied to sensitive assets, depending on the degree of sensitivity involved:

TOP SECRET
SECRET
OFFICIAL

Definitions:

OFFICIAL:
ALL routine police (and wider public sector) information assets should be treated as OFFICIAL. This includes a wide range of information, of differing value and sensitivity, which needs to be defended against compromise by attackers with bounded capabilities and resources. The threat profile may include (but is not limited to) hacktivists, single-issue pressure groups, investigative journalists, competent individual hackers and the majority of criminal individuals and groups. The need-to-know principle still applies to any OFFICIAL content.

The following HMG information will generally be regarded as OFFICIAL:

- The day-to-day business of government, service delivery and public finances.
- Routine international relations and diplomatic activities.
- Public safety and criminal justice.
- Enforcement, incident records, and investigation activities.
- Many aspects of defence, security and resilience.
- Commercial interests, including information provided in confidence and intellectual property.
- Personal information that is required to be protected under the Data Protection Act (2018) or other legislation.

The vast majority of information assets dealt with by NYP employees will be classified as OFFICIAL. The definitions of SECRET and TOP SECRET are included for completeness but are not discussed in detail within this procedure document.

SECRET:
Very sensitive information that requires protection against highly capable threat actors (i.e., sophisticated, well-resourced, and determined threat actors, such as some highly capable serious organised crime groups and some state actors) AND where the effect of accidental or deliberate compromise would be likely to result in any of the following:

a) Directly threaten an individual's life, liberty, or safety (from highly capable threat actors).

b) Cause serious damage to the operational effectiveness or security of UK or allied forces such as
i) that in the delivery of the Military tasks:
ii) Current or future capability would be rendered unusable;
iii) Lives would be lost;
iv) Damage would be caused to installations rendering them unusable.
v) Cause serious damage to the operational effectiveness of highly valuable security or intelligence operations.

c) Cause serious damage to relations with friendly governments or damage international relations resulting in formal protest or sanction.

d) Cause serious damage to the safety, security or prosperity of the UK or friendly nations by affecting their commercial, economic, and financial interests.

e) Cause serious damage to the security and resilience of Critical National Infrastructure (CNI) assets.

f) Cause major impairment to the ability to investigate or prosecute serious organised crime.

TOP SECRET:
Exceptionally sensitive Government (or partner's) information assets that directly support (or threaten) the national security of the UK or allies AND require extremely high assurance of protection from all threats. This includes where the effect of accidental or deliberate compromise would be likely to result in any of the following:

a) Lead directly to widespread loss of life.

b) Threaten directly the internal stability of the UK or friendly nations.

c) Raise international tension.
d) Cause exceptionally grave damage to the effectiveness or security of the UK or allied forces, leading to an inability to deliver any of the UK Defence Military Tasks.

e) Cause exceptionally grave damage to relations with friendly nations.

f) Cause exceptionally grave damage to the continuing effectiveness of extremely valuable security or intelligence operations.

g) Cause long term damage to the UK economy.

h) Cause major, long-term impairment to the ability to investigate or prosecute serious organised crime.

How to record

When applying a protective marking to a document, the security marking (e.g., OFFICIAL-SENSITIVE, SECRET or TOP SECRET) will be displayed in capital letters, centred in the header and footer of a document.

Protective marking of OFFICIAL assets
There is no requirement to routinely apply a visible marking to OFFICIAL documents. **A document which has no visible marking is assumed to be OFFICIAL.** The lack of a visible marking does not mean that an asset does not require protection. Staff must be aware that **ALL HMG information must be handled with care to prevent loss or inappropriate access and deter deliberate compromise or opportunist attack.**

The OFFICIAL-SENSITIVE caveat marking
A limited subset of OFFICIAL assets could have more damaging consequences if it were lost, stolen, or published in the media. For example, if these assets were compromised, this may put individuals at risk of harm, cause disruption to ongoing investigations or damage the reputation of the police service.

This subset of information should still be managed within the OFFICIAL classification tier but may attract additional measures. **In such cases where there is a clear and justifiable requirement to reinforce the 'need to know', assets must be conspicuously marked: OFFICIAL–SENSITIVE.**

The marking of assets as "OFFICIAL-SENSITIVE" must be applied sparingly on a case-by-case basis; it may not be necessary for sensitive OFFICIAL information that is already managed through clear and well understood business processes and where there is no requirement or benefit for this sensitivity to be explicitly highlighted through an additional marking.

When applying the OFFICIAL-SENSITIVE marking, the originator **must** also state why they have marked it "OFFICIAL-SENSITIVE" and must also apply handling conditions and network control measures for example additional security protection in its transmission such as encryption. This

applies to not only files and documents that you are intending to share, but also those that are held by the organisation in records management systems, SharePoint Libraries, and any other storage repositories. Applying the OFFICIAL-SENSITIVE marking to content within an email does not automatically improve the security of the communication transmission. You should refer to the Secure Communication of Police Data guidance for further clarity on how to secure the information in transit.

The following is an example of how the OFFICIAL–SENSITIVE marking is applied:

Example:

OFFICIAL-SENSITIVE: OPERATIONAL

The contents of this email contain sensitive personal information. Do not disclose or disseminate to others without firstly seeking permission from the originator. If authority to share has been agreed, it must be shared via secure e-mail.

Examples of OFFICIAL-SENSITIVE assets

The following list provides some examples of police information which may require marking as OFFICIAL-SENSITIVE. This is not in any way intended to be an exhaustive list:

- Intelligence Sources;
- Covert or sensitive police tactics and operations;
- Personal details of staff working in sensitive roles;
- Special category data as defined under the Data Protection Act 2018 (e.g., criminal offence data, health data, religious beliefs, Trade union membership)
- Staff misconduct or corruption;
- Multi Agency Public Protection Arrangements (MAPPA) and ViSOR records;
- High profile cases (for example, prosecutions involving public figures);
- Vulnerable victims and witnesses (e.g., serious harm, violence and sexual investigations, victims fleeing domestic abuse, threat to life incidents, intimidated witnesses and Witness Protection arrangements);
- Documentation protected by Legal Professional Privilege.

The use of "OFFICIAL" as a security marking

In some limited circumstances, the originator may wish to apply a GSC marking to an OFFICIAL document that is not considered particularly sensitive and would not meet the threshold for "OFFICIAL-SENSITIVE" marking. In such circumstances, it is possible for OFFICIAL to be used as a protective marking, but the originator must also state **why** they are marking the document and **conside**r specifying handling conditions.

For example, where a document is circulated for peer review prior to being openly published, the originator may apply the following marking:

Example:

OFFICIAL

This document is for recipients only. Not to be circulated prior to 1st June.

The use of OFFICIAL as a protective marking must only be used by exception when the originator considers it is necessary to highlight a particular issue or circumstance. In the above example, it

would also be acceptable for the originator to conspicuously write the handling conditions within the body of the document without using OFFICIAL as a marking. If no GSC classification was displayed, it would be assumed to be OFFICIAL.

Descriptors

When marking an asset as OFFICIAL-SENSITIVE, a DESCRIPTOR must* also be applied to help indicate to others the nature of the sensitivity. One of the following four descriptors must be used:

OPERATIONAL - to support ongoing sensitive investigations or operational security matters
PERSONNEL - personal occupational health/medical records, sensitive staff matters
COMMERCIAL - matters between organisations and suppliers
ORGANISATIONAL - matters that do not fit any of the above

If the originator wishes to mark a routine asset as OFFICIAL, use of a descriptor is optional.

*Note that the use of the above descriptors for sensitive assets is NYP policy only. Other organisations may not mandate use of descriptors or may use different descriptors. When communicating with overseas bodies, descriptors should not be used without prior agreement as they are not internationally recognised and may cause confusion.

A further optional descriptor can be applied by the originator if desired, for example the name of an operation:

Example:

OFFICIAL-SENSITIVE: OPERATIONAL – OP RAINBOW

It is the user(s) responsibility to ensure they allocate the necessary GSC marking to suit the sensitivity within the information and or data, which will support their decision making to select the necessary level of security and communication type to transfer Police information.

Before sending ANY communications, please self-assess:

- 'WHAT' information you are sending, and the risks associated to the organisation if the information should be exposed, revealed, or lost and the likelihood of this happening.
- 'WHO' you are sending the communications to
- 'HOW' you are sending the communications

Further information can be found in the Secure Communication of Police Data Guidance

Handling of historic protectively marked documents
Historic documents that display a GPMS marking do not need to be amended to show a GSC marking unless there is an identified need or benefit to doing so. Documents such as crime files carrying a GPMS marking should continue to be handled as they were previously.

Assets such as policies, procedures, templates, forms, and IT systems should be updated to comply with GSC at a natural review date alongside other necessary or planned changes.

Freedom of information act and subject access requests

A Protective Marking cannot prevent disclosure following a Freedom of Information Act (FOIA) or Subject Access Request (SAR), nor can its absence automatically mean disclosure. An assessment is made on a case-by-case basis regarding the disclosure of information or whether an exemption applies.

Legal Professional Privilege
Marking a document as being subject to Legal Professional Privilege does not mean that Legal Professional Privilege will not be waived, if the conditions for waiving privilege are made out i.e., Disclosure of a privileged document to a third party. If you are unsure whether a document is subject to Legal Professional Privilege you should obtain advice from Joint Corporate Legal Services.

Information sharing
The release of sensitive information to other organisations (for example, other police forces or partner agencies) will depend on their ability and willingness to protect the information. The level of protection required by the Protective Marking and accompanying handling conditions of an information asset shall be upheld by any organisation it is disclosed to.

Under no circumstances can information assets be disclosed if the potential recipients are unwilling or unable to meet the security requirements of the GSC classification and/or the accompanying handling caveats. Wherever possible, regular sharing of sensitive information should be supported by an Information Sharing Agreement (refer to Information Sharing Procedure).

It is important to note that sharing of any information with outside agencies must only take place where the Data Protection Act (DPA) permits and that a protective marking (or lack thereof) cannot override or prevent a breach of the DPA. Refer to Data Protection Procedure for further guidance.

The Protective Marking of a document can diminish or even increase over time. It is therefore necessary to consider the life expectancy of a Protective Marking given to a document. For example, if a member of the Royal Family is visiting North Yorkshire, the risk assessment, and tactical plans for protecting the visitor may be classified to SECRET. However, once the visit has passed, this may drop to OFFICIAL-SENSITIVE as the impact of the information assets has diminished, but unauthorised disclosure may expose guarded tactics which could cause damage to the effectiveness of valuable security or intelligence operations in the future.

The recipient of information carrying a Protective Marking shall:
Challenge the Protective Marking of a document if they believe that an incorrect Protective Marking has been used. Only the originator of a document can change the Protective Marking, hence, they should be contacted and constructive reasoning to change the marking of the document/ information should be given.

All staff must protect and use the document/information in accordance with the Protective Marking required and any supplemental instructions.

Responsibilities

Operational Officers/Police Staff

The Protective Marking of a document is applied by the originator (in most cases the creator) and may only be changed with the originator's authority unless under exceptional circumstances. The originator must:

- consider to what classification the document must be protected, the higher the classification, the greater administrative burden on the organisation and the smaller the circulation of the document
- consider if additional handling conditions and network controls need to be specified to accompany the protective marking. For OFFICIAL-SENSITIVE marking, handling conditions MUST be specified.
- consider the duration of the classification, or review period

Staff handling protectively marked material must:

- ensure that material is appropriately stored, transferred or transmitted in accordance with minimum standards as specified in the **Appendix A - Information Asset Control Measures**.
- abide by any additional handling conditions and network controls specified by the originator
- consider constructive feedback as to the classification of a document and/or handling conditions attached to document. Originators have the responsibility of setting a classification and, if appropriate, changing the classification and/or handling conditions

First Line Supervision

In addition to the above, Line Managers are responsible for ensuring staff mark material correctly. Staff can be helped by developing guidance specific to their own areas of operation. The following measures should be introduced:

- identify and support relevant training needs of staff, in particularly ensuring that any mandatory training packages on GSC are completed
- oversee and facilitate full compliance with information asset control measures for GSC including, ensuring staff are appropriately security vetted and suitable equipment is available (e.g., lockable cabinets) ensuring that any use of the "OFFICIAL-SENSITIVE" marking is necessary, appropriate, and implemented correctly as defined in this procedure document
- emphasising that documents should not necessarily be given the same marking as those to which they are attached, refer, or respond giving parts of a document, e.g., individual paragraphs, different Protective Markings (e.g., marking parts of OFFICIAL documents as OFFICIAL-SENSITIVE)
- putting time limits on markings or documents to ensure protective measures are not applied for longer than necessary
- limiting the marking on a document by extracting sensitive information into an appendix so that the main text can be distributed separately and more widely

Safer Neighbourhood Commanders/Heads of Functions/ Information Asset Owners

In addition to the above, Safer Neighbourhood Commanders, Heads of Functions and Information Asset Owners must ensure staff and officers are aware of, and comply with, the Force Protective Marking Procedure and its inclusion within any Information Sharing Agreements.

Chief Officer Team

Overall responsibility for the security of all information assets.

The Protective Marking system operates on the fundamental basis of the “need to know” principle. In order to access higher levels of classification, staff must have sufficient security clearance.

Definition of Special Terms

APP - Authorised Professional Practice

GSC - Government Security Classification

MoPI - Management of Police Information

NPCC - National Police Chiefs’ Council

Note: In compliance with the Freedom of Information Act all force policies and procedures that are not marked as OFFICIAL-SENSITIVE will be published on the NYP Website. It is necessary to apply Government Security Classification (GSC) see Protective Marking Procedure for advice on how to mark and handle documents.