



POLICY



Policy Title: GOVERNMENT SECURITY CLASSIFICATION

Table of Contents

Section 1 - Introduction.....	1
Section 2 - Purpose	1
Section 3 - GSC Guidance Handout	2
Section 4 - General Principles of the Policy	2
Section 5 – Need-to-Know Principle.....	3
Section 6 - Implementing the GSC	3
Section 7 - OFFICIAL classification.....	3
Section 7.1 - Marking a document as OFFICIAL.....	3
Section 7.2 - Marking a document as OFFICIAL - SENSITIVE	4
Section 7.3 - SECRET Classification	4
Section 7.4 - TOP SECRET Classification	5
Section 8 - Handling Instructions.....	5
Section 9 - Storage	5
Section 10 - Disposal.....	5
Section 11 – Sending via E-mail	5
Section 12 - Clear Desk and Clear Screen Policy.....	5
Section 13 - Supporting Documentation.....	5
Section 14 - Legal Basis.....	5
Appendices	6

Section 1 - Introduction

It is the policy of the Chief Constable for Gloucestershire and the Office of the Police and Crime Commissioner (OPCC) to provide guidance for all employees to utilise the HMG Government Security Classification (GSC) policy in respect of its information and to allocate appropriate markings according to the sensitivity of the information on systems and documents.

This policy applies to all employees of Gloucestershire Constabulary and OPCC staff which include those who are on part time, fixed term, or permanent contracts and those on secondment, applies to volunteers, consultants and delivery partners.

The new GSC has replaced the existing Government Protective Marking Scheme (GPMS) and will adopt it from the 3 April 2017 when the GSC must be applied to any new documents that are produced and will be required to apply retrospectively to existing documents by October 2018. During the reviewing process of documents this policy must be implemented.

Section 2 - Purpose

The purpose of this policy is to ensure that Gloucestershire Constabulary and OPCC comply with the requirements of the GSC and to provide instruction for the marking and handling of information.

Everyone who works within the Constabulary has a duty to respect the confidentiality and integrity of all information and data that they access, and is personally accountable for safeguarding information assets in line with this policy.

This policy provides a framework for classifying information, and directs users to particular levels of control which are required to ensure the continuing Availability, Integrity and Confidentiality of information. The criteria for determining the correct classification must consider both the level of threat posed to the information and the impact it would have should the information be compromised.

This policy describes how the Constabulary classify Information Assets to ensure they are appropriately protected and supports policing business processes by ensuring the value of information to the Constabulary is fully exploited. The policy applies to all the information that each Force collects, stores, processes, generates or shares to deliver services and conduct the business of policing, including information received from or exchanged with other Police Forces and third party suppliers.

The GSC is intended to make it easier to classify information in a more meaningful way; improve sharing within government and with external partners, CPS etc; making sure that sensitive information receives the protection it needs.

This document should be read in conjunction with GSC guidance leaflet which provides advice on Handling, Storage and Movement of GSC marked material, Appendix A.

This Policy should enable consistent and effective decision making. Where operational or managerial circumstances require any decision making that would adversely affect adherence to the policy or procedure, in line with the 'Statement of Intent' of the constabulary and the police service 'Code of Ethics', if an officer/ police staff member believes that they need to make a decision that steps outside of policy and procedure they should do so, provided that:

- The officer/ police staff member raises the matter at the earliest opportunity (and ideally before any such decision is made) with their line manager declaring their intended (or actual) course of action if notification is made after the decision is taken,
- Produces, in a timely manner, a signed and dated written explanation of why it is/ was deemed necessary to step outside of policy and procedure, and
- Maintain an adequate record of this written rationale for audit purposes appropriate to the circumstances/ contravention

Section 3 - GSC Guidance Handout

Classification applies to all sensitive information irrespective of how it is held. It applies to documents including memos, letters, reports, project papers, tenders, contracts, financial information and includes electronically held documents.

This applies to all printed material whether originating from within the Constabulary or received from another Constabulary or outside origination / agency.

Each classification requires a minimum set of security controls, to be in place to provide the appropriate protection against a range of threats which are explained in the GSC Guidance Handout, Appendix A & B.

Section 4 - General Principles of the Policy

This policy supports the proposed Constabulary's Information Management Strategy (IMS) which sets out the Constabulary's commitment to the management of police information and what police personnel and delivery partners / third party suppliers should do to manage police information. In doing so, this policy also supports the Constabulary's Force Strategic aims and objectives and should enable employees throughout the organisation and external support personnel, to identify an acceptable level of risk and use appropriate handling controls.

All information that the Constabulary needs to collect, store, process, generate or share to deliver services and conduct police business has intrinsic value, and all staff must apply the appropriate degree of protection.

Any breach of the rules contained within this Policy could result in an investigation.

Staff must risk assess sharing information and only share information with those who have a legitimate requirement to see it. Information can be shared only on the basis of a genuine need to know.

Section 5 – Need-to-Know Principle

The dissemination of sensitive information and assets should be no wider than is necessary for the efficient conduct of Gloucestershire Constabulary and, by implication, should be limited to those individuals who are appropriately authorised to have access to it. This “need to know” principle is fundamental to the protection of our sensitive data/assets. It applies both within the Constabulary or agency and when dealing with individuals outside of it.

Section 6 - Implementing the GSC

The GSC classification system has three levels: OFFICIAL (including OFFICIAL – SENSITIVE), SECRET and TOP SECRET.

Each classification requires a minimum set of security controls, to be in place to provide the appropriate protection against a range of threats.

Security classifications indicate the sensitivity of information (in terms of the likely impact resulting from compromise, loss or misuse) and the need to defend against a broad profile of applicable threats. There are three levels of classification:



The Classifications do not have any direct implications for access to information under either the Data Protection Act (1998) or the Freedom of Information Act (2000).

Classification markings can assist in assessing whether exemptions to the DPA or FOIA may apply. However, it must be noted that each request must be considered on its own merits and the classification in itself is not a justifiable reason for exemption, the same is true should the document not have marking, it would not be assumed that the information can automatically be disclosed.

Section 7 - OFFICIAL classification

All documentation originated by the Constabulary is classed as OFFICIAL even without the marking.

The OFFICIAL classification reflects the fact that reasonable measures need to be taken to look after an Information Asset and to comply with relevant legislation such as the Data Protection Act.

The controls in place must be sufficient to protect against a range of impacts and threat actors such as hacktivists, single issue pressure groups, investigative journalists, competent individual hackers, and the majority of criminal individuals or groups.

All staff should apply this policy and ensure that consistent controls are implemented throughout the police service, delivery partners and wider supply chain. Delivery partners and suppliers who have access to the Constabulary information must apply equivalent controls, which should be provided for under contractual provisions or Information Sharing Agreements.

Section 7.1 - Marking a document as OFFICIAL

Documents are to be marked OFFICIAL when it includes the following:

- Non-policing services, some of which could have damaging consequences if lost, stolen or published in the media, but are not subject to a heightened threat profile.
- General day to day policing activity.
- Most front line service operations.
- Organisation and performance management information.
- Personal information (including staff data, case files, HR or medical records).
- Business information (finance, estates, personnel, policy, commercial).

Section 7.2 - Marking a document as OFFICIAL - SENSITIVE

A limited amount of OFFICIAL information could have more damaging consequences if lost, stolen or published in the media. This subset of information should still be managed within the OFFICIAL classification, but as it has a higher impact if compromised should attract additional control measures (generally procedural or personnel), to reinforce the 'need to know' principal.

In these cases where there is a clear and justifiable requirement, then information can be described using the caveat of SENSITIVE i.e. **OFFICIAL - SENSITIVE**.

This more sensitive information must be identified by being marked OFFICIAL - SENSITIVE. This marking alerts users to the enhanced level of risk and that additional controls are required, examples below:

- Detrimental impact on an investigation.
- Cause a risk to Life and/or safety.
- Breaching legislation restrictions (DPA).
- Have an impact on security or intelligence led operations.
- Have a detrimental impact on the Constabulary or police service.

A handout has been produced to help users apply the various requirements for handling documents OFFICIAL & below, which is at Appendix A, which is published on the Constabulary's intranet, inSIGHT.

Section 7.3 - SECRET Classification

The SECRET classification must only be used where there is a high impact of risk and a sophisticated / determined threat from such elements as serious and organised crime and foreign intelligence services.

Examples of SECRET include:

- Classified material received from Government Departments / agencies relating to National Security and Counter-Terrorism
- Intelligence and investigations relating to individuals of interest to security agencies
- Information that could cause serious damage national security and intelligence operations
- Information affecting the ability to investigate or prosecute serious/organised crime where there is intelligence to suggest there is a known sophisticated and determined threat to access the information
- Personal/case details where there is a specific threat to the life/liberty of an individual such as protected witness scheme records.

The concept of sophisticated or heightened threat does not only apply to those with a high technical (e.g. IT) attack capability. It can apply to criminals who have a developed capability to intimidate or coerce individuals i.e. if disclosure of information could result in serious physical harm or put a life at risk because there is a real and highly capable threat present, the information must be tightly controlled.

SECRET must not become the default status for material just because of the type of case or potentially severe consequences (e.g. murder trials, or where there is a threat to life). The threat capability must also be present. There is no change to controls at this level.

Guidance for handling documents marked SECRET or TOP SECRET has been written, Appendix B

Section 7.4 - TOP SECRET Classification

This classification remains for information of the highest sensitivity relating to national security and subject to highly capable threat sources. There is no change to controls at this level.

Guidance for handling documents marked SECRET or TOP SECRET has been written, Appendix B.

Section 8 - Handling Instructions

Handling instructions are to provide additional measures on how you want the recipient/s to manage the document or email that you have shared and can be added by the author/originator to any OFFICIAL or OFFICIAL-SENSITIVE document.

They must be added to all documents marked OFFICIAL-SENSITIVE. They can detail what network must be used, include how to store the information, you can add any restrictions on further distribution and disposal methods etc, see below:

- For named recipient/s or distribution group
- Secure e-mail addresses only
- No copying/printing/sharing of material without the author's approval
- Files to be deleted when work completed
- Not to be shared outside Gloucestershire Constabulary

Section 9 - Storage

The following should be considered when storing OFFICIAL paper documents:

OFFICIAL, storage under single barrier and/or lock and key

OFFICIAL – SENSITIVE, in secure cabinets under double barrier, a locked container in a locked room.

Section 10 - Disposal

All OFFICIAL paper documents must be disposed destroyed by a cross cut shredder or placed in secure waste sacks/bins provided until collected for destruction.

Section 11 – Sending via E-mail

The internal e-mail messaging system is accredited to transmit protectively marked information up to OFFICIAL, which includes OFFICIAL-SENSITIVE marked material.

If you are sending a protectively marked e-mail externally you are to ensure that the recipient's e-mail address is secure. These addresses and further advice can be found in the e-mail security policy.

If there is a requirement to send an e-mail to a non-secure e-mail address, which could prevent a threat to life then you can send but record your justification.

Section 12 - Clear Desk and Clear Screen Policy

Information left out on desks is vulnerable to compromise and likely to be damaged or destroyed in the event of a disaster such as fire, flood or explosion. Therefore, all official information and removable storage media should be removed from desk surfaces when not in use, particularly prior to an employee's departure from Constabulary premises each evening.

Section 13 - Supporting Documentation

This policy must be read in conjunction with any specific instructions issued for each information facility and the following supporting documentation:

- Information Security policy
- Internet Security policy
- E-Mail Security policy

Section 14 - Legal Basis

Supported by legislation including:

- Official Secrets Acts 1989
- Data Protection Act 1998
- Computer Misuse Act 1990
- Freedom of Information Act 2000
- Code and Guidance on the Management of Police Information
- Security Policy Framework

Appendices

Appendix A – Guidance handout for marking and handling documents OFFICIAL & below.

Appendix B – Guidance for handling documents marked SECRET or TOP SECRET

Security Marking:		None	
Document Title: POLICY			
GOVERNMENT SECURITY CLASSIFICATION POLICY			
Type		URN	Strategic Board
Policy		261	Information Governance Board
Author/Reviewer		Steve Davis. IGB members	
Version	Date	Changes (ensure public copy amended and uploaded to external website)	
		Complied with Policy Guidance ✓	
0.6	8 Dec 16	Initial draft for review	
0.7	20 Dec 16	Inserted comments from DPO	
0.9	5 Jan 17	Inserted comments from GSC working group	
1.0	25 Jan 17	Approved by GSC working group	
1.0b	22 Feb 17	Minor changes	
Next Document Review Date:			
EIA		EIA Sign Off	EIA Review
LOW/MEDIUM/HIGH			
SIA		SIA Sign Off	SIA Review
<i>This version will be placed on the public domain website</i>			
If this version cannot be placed on the public domain website, provide reason and relevant COG authority			