

HANDLING OF PROTECTIVELY MARKED MATERIAL

A Guide on Security Markings for Counsel

July 2018

Author: Simon Harker
GLD

Introduction

You may from time to time be instructed on matters that carry a security restriction. If you are instructed it is possible that you will receive a more detailed note setting out how security marked material should be handled. However, whether or not you do, if you receive security marked material and are in any doubt about what to do then please contact the case holder.

Since April 2014 the main restrictions used by Government Departments are OFFICIAL, SECRET and TOP SECRET. However you may come across the pre April 2014 classifications of PROTECT, RESTRICTED, and CONFIDENTIAL. If you want to know how to handle these documents refer to the previous edition of this Guide.

Only Counsel that have been Security Checked (SC'd) or Developed Vetted (DV'd) will be asked to deal with SECRET or TOP SECRET work. If you are not SC'd or DV'd and you do receive any material marked SECRET and TOP SECRET, you should contact the person who has sent you this material immediately to make arrangements for its collection, should hold it securely pending collection and should not read it. If special arrangements are made for you to read such material without full clearance, you will be informed of that.

Documents that would previously have been marked PROTECT, RESTRICTED, CONFIDENTIAL would now be classified OFFICIAL.

You should read this Guide in conjunction with the revised "Attorney General's Guidelines on Information Security and Government Work" produced by GLD), the CPS and Whitehall Prosecuting Departments in conjunction with the Bar Council setting out agreed common standards for material marked Official. A copy is on the GOV.UK website. **This document is referred to in this document as the "Guidelines".**

OFFICIAL

“Official” Information should be held, processed, transmitted or transported, and destroyed with discretion, in order to avoid unauthorised access.

- **Storage**
See the Guidelines
- **Control /Transmission**
See the Guidelines

NB

- Copies should be kept to a minimum.
 - Information with a protective marking of Official must **not**, under any circumstances be transmitted over the Internet. However, it may be transmitted via the Criminal Justice Secure email. See the separate Guidance on use of CJSM.
 - Avoid the use of FAX. If it has to be used then keep sensitive details to a minimum.
 - Items transmitted within a single building should be sent by trusted hand or in a transit envelope. Between different sites, items should be sent in a sealed envelope/container by hand or by postal/DX service addressed to an individual by name or appointment. The cover should show no marking.
- **Computers**
See the Guidelines
 - **Disposal/Destruction**
See the Guidelines

'OFFICIAL-SENSITIVE'

There is a limited subset of "Official" information that could have more damaging consequences (for individuals, an organisation or government generally) if it were lost, stolen or published. This subset of information is still to be managed within the 'OFFICIAL' classification tier, but may attract additional security measures (generally procedural or personnel) to reinforce that only those who 'need to know' should have access. For example an '**OFFICIAL-SENSITIVE**' document might have the instructions

HAND DELIVERY ONLY.

This document must not be sent by postal or courier services.

It is important to note that **OFFICIAL - SENSITIVE** is not an additional classification. In addition by the time you receive such documents in your bundle of papers, any instructions about handling such documents over and above those required by the simple "OFFICIAL" category are likely to be otiose. You should therefore treat "Official -Sensitive" documents in the same way as any other "Official" document unless that document is an original one that contains instructions specifically addressed to you.

SECRET

The Secret marking is used for example when compromise of the information would directly threaten life e.g. terrorist cases, cases naming police informants or threats to witnesses, etc.

It is used when accidental or deliberate compromise is likely to:

Threaten life directly or seriously prejudice public order, individual security or liberty

Cause substantial material damage to national finances or economic and commercial interests

Raise international tension

Affect the defence of the UK

Secret information and other assets should be held, processed, transmitted or transported and destroyed under conditions which make it highly unlikely that compromise and those responsible will go undetected.

- **Storage:**
 - Documents and laptops (see further below) must be kept in security containers. For GLD work, the case officer at GLD will arrange for you to receive the appropriate security container.
 - No working on papers outside Chambers e.g. at home or in a hotel
- **Control/Transmission:**

Documents must not be removed from Chambers without written permission from your Instructing Solicitor.

No fax, telephone, e mail or photocopying

Items to be carried only by trusted hand, approved courier or Royal Mail Special Delivery Service in a secure container or double covers. A receipt **must** be obtained. **Documents passing between London Chambers and GLD's offices at OKS must go by hand.**

Outer covers should show no marking but **must** include recipient's name **and/or** appointment, address and a return address. Inner covers must be similarly addressed and clearly marked **Secret**.
- **Computers**

Work must be done on Government supplied computers. For GLD work the case worker at GLD will arrange for you to receive one for the duration of the case. Instructions on the use of that computer will be given to you. No use of USB sticks
- **Disposal/Destruction:**

All material that has been used for protected data should be subject to controlled disposal. Discuss with the case holder.

TOP SECRET

The Top Secret marking is used for example when compromise of the information directly would be likely to lead to widespread loss of life, e.g. Terrorist cases.

Would accidental or deliberate compromise be likely to:

Lead directly to widespread loss of life?

Threaten directly the internal stability of the UK or friendly nations?

Cause severe long-term damage to the UK economy?

Affect the defence of the UK?

Top Secret information and other assets should be held, processed, transmitted or transported and destroyed under conditions which **ensure** actual or attempted compromises will be detected and those responsible will be identified.

- **Storage:**
 - Documents and laptops (see further below) must be kept in security containers. For GLD work, the case officer at GLD will arrange for you to receive the appropriate security container.
 - No working on papers outside Chambers e.g. at home or in a hotel
- **Control/Transmission:**
 - Documents must not be removed from Chambers, without written permission from your instructing solicitor.
 - No Fax, telephone, e mail or photocopying.
 - Items to be carried only by trusted hand, approved courier or Royal Mail Special Delivery Service in a secure container or double covers. A receipt **must** be obtained. **Documents passing between London Chambers and GLD's offices at OKS must go by hand.**
 - An approved tamper evident envelope/secure container **must** be used as an outer cover to include recipient's name **and/or** appointment, address and return address. Inner covers **must** be similarly addressed and clearly marked Top Secret, To Be Opened By (addressee only, or return to sender).
- **Computers**

Work must be done on Government supplied computers and for GLD work the case worker will arrange for you to receive one for the duration of the case. Instructions on the use of that computer will be given to you. No use of USB sticks.
- **Disposal/Destruction:**

All material must be subject to controlled disposal. Discuss with the case holder.