HANDLING OF PROTECTIVELY MARKED MATERIAL

A Guide on Security Markings for Counsel

July 2011

Author: Simon Harker
TSol

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.

The main restrictions used by Government Departments are RESTRICTED, CONFIDENTIAL, SECRET and TOP SECRET. 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.

These are markings to be contrasted with the sub-national security marking of PROTECT which is in use by some Departments to protect personal information relating to named individuals.

It may be that as well as receiving protectively marked documents you also create them i.e. you produce pleadings or produce a marked up version of a witness statement. If you produce a new document that needs a protective security marking then you should apply the appropriate markings in bold font, the same size as body text, aligning the centre, at the top and bottom of each page or in the header and footer. In assessing whether to use a marking, you should always consider, how damaging the consequences would be if the material was lost, stolen, disclosed or destroyed. Please try to apply the correct marking as both over and under-classification damage the credibility of the system.

You should read this Guide in conjunction with the "Attorney General's Guidelines on Information Security and Government Work" produced by TSol, the CPS and Whitehall Prosecuting Departments in conjunction with the Bar Council setting out agreed common standards for material at PROTECT or RESTRICTED levels. A copy is on the TSol website. **These are referred to in this document as the "Guidelines".**

1. Protect

The PROTECT marking safeguards information that links one or more identifiable living persons with information about them whose release would put them at significant risk of harm or distress. The following chart is extracted from Cabinet Office guidance.

A.

1. one or more of the pieces of information which can be used along with public domain information to identify an individual	**combined with**	**2. information about that individual whose release is likely to cause harm or distress**
Name / addresses (home or business or both) / postcode / email / telephone numbers / driving licence number / date of birth [Note that driving licence number is included in this list because it directly yields date of birth and first part of surname]		Sensitive personal data as defined by s2 of the Data Protection Act, including records relating to the criminal justice system, and group membership DNA or finger prints / bank, financial or credit card details / National Insurance number / Tax, benefit or pension records / health records / employment record / school attendance or records / material relating to social services including child protection and housing

.

B. Any source of information about 1000 or more identifiable individuals, other than information sourced from the public domain.
This could be a database with 1000 or more entries containing facts mentioned in the box above, or an electronic folder or drive containing 1000 or more records about individuals. Again, this is a minimum standard. Information on smaller numbers of individuals may warrant protection because of the nature of the individuals, nature or source of the information, or extent of information“

When considering whether release or loss would put someone at significant risk of harm or distress a good rule of thumb is whether the information would have a cash value if it fell into the wrong hands e.g. details of someone’s bank account. A letter that contained an individual’s National Insurance Number would have a cash value to a criminal and its misuse could cause financial harm to the individual. It is therefore protected personal data. A letter that simply referred to a named individual breaking his leg has no financial value and therefore is not protected personal data.

Equally when it comes to information about an individual’s employment, the key is whether the release or loss of the information would cause harm or distress. A letter indicating that someone works for a named company which experiments on animals is protected personal data because the individual could suffer harm if it fell into the hands of violent anti vivisectionists. Information that someone works for the Civil Service is not.

NB You should be aware the PROTECT marking is also used by some Departments for documents that would be likely to:

- Breach proper undertakings to maintain confidentiality of information provided by 3rd parties
- Breach statutory restrictions on the disclosure of information

- **Storage**
  See the Guidelines

- **Control/Transmission**
  See the Guidelines
  NB keep photocopying to a minimum

- **Computers**
  See the Guidelines

- **Disposal/Destruction:**
  See the Guidelines

2. <u>Restricted</u>

Applied when accidental or deliberate compromise is likely to:

Cause substantial distress to individuals

Cause financial loss or loss of earning potential or facilitate improper gain or advantage to individuals/companies

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

Disadvantage government in commercial or policy negotiations with others

Undermine the proper management of the public sector and its operations

Restricted information and other assets 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 **Restricted** or above must **not**, under any circumstances be transmitted over the Internet. However, Information with a protective marking of **Restricted or below** 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

2. <u>Confidential</u>

Applied when accidental or deliberate compromise is likely to:
Prejudice individual security or liberty
Work substantially against national finances or economic and commercial interests
Impede the investigation or facilitate the commission of serious crime
Seriously impede the development/operation of major Government policies
Shut down or substantially disrupt significant national operations

Confidential information and other assets should be held, processed, transmitted or transported and destroyed under conditions which inhibit casual or wilful unauthorised access and are likely to assist in the identification of compromises.

- **Storage:**

    - Documents and laptops must be kept in security containers. For TSol work, the case officer will arrange for you to receive the appropriate security container.

    - No home working without permission.

- **Control/Transmission:**

    No fax, e mail or photocopying. Use the telephone with discretion.

    Items transmitted within a single building should be sent by trusted hand or in a sealed envelope. Between sites items should be sent in a sealed envelope/container or by postal/DX service addressed to an individual by name or appointment. The cover should show no marking.

    Double covers must be used if sent to a non-Government address; the outer cover should show no marking but must include recipient's name and/or appointment, address and a return address. Inner covers should be similarly addressed and clearly marked Confidential.

    - **Computers**
      See the Guidelines but no USB sticks

    - **Disposal/Destruction:**
      See the Guidelines.

3. 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 TSol work, the case officer at Treasury Solicitors 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 TSol'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 TSol work the case worker at Treasury Solicitors 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.

4. <u>Top Secret</u>

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 TSol work, the case officer at Treasury Solicitors 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 TSol'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 TSol 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.