25.6.10

GUIDELINES ON INFORMATION SECURITY AND GOVERNMENT WORK

Introduction and the Application of these Guidelines

1. These Guidelines have been produced following the response of various Government Departments and Agencies to the requirements of the Information Security and Assurance of HMG Security Policy Framework[1] issued by the Cabinet Office in December 2008. These Guidelines deal only with the steps which barristers should take to meet the particular requirements of Prosecution and other United Kingdom Government agencies. They have been prepared by the relevant Government Departments in conjunction with the Bar Council. Although they do not apply to information provided to barristers by other clients, you are requested to have these Guidelines in mind when dealing with Restricted information which may have originated from Government Departments and Agencies.

Categories of Information

2. Material supplied to counsel falls into different categories of sensitivity:

(a) Many documents routinely supplied to counsel acting for Prosecution or other Government agencies fall into the Restricted or Protect categories. The designations Restricted and Protect (as used by Government agencies) include material the accidental release of which may cause substantial distress to individuals, breach proper undertakings to maintain the confidence of information provided by third parties, or prejudice the investigation of or facilitate the commission of crime. Examples could include personal data such as copies of bank statements, and the personal, medical or financial details of defendants, victims or witnesses. The data may also provide information concerning current investigations.

(b) Government agencies use the designations Confidential, Secret and Top Secret to refer to more sensitive material. The nature of such material varies greatly, and encompasses material covered by Public Interest Immunity, family and child abuse documents, as well as information dealing with national security issues of varying degrees of complexity and sensitivity.

3. Except where stated otherwise, these Guidelines do not apply to material which should be regarded as being more sensitive than Restricted. The identification, treatment and handling of this more sensitive material will be determined by the instructing solicitor, prosecution agency or relevant Government department. The security requirements for such more sensitive material will vary according to the nature of each case, the type of material held and, where appropriate, may be a matter for discussion with counsel. Some Government Departments provide counsel with safes, secure dedicated laptops, photocopiers and printers, and physical escorts for the transfer of such material to courts or tribunals. Other forms of more sensitive material may require less stringent security measures.

---

[1] *HMG Security Policy Framework:* Cabinet Office, December 2008: http://www.cabinetoffice.gov.uk/media/111428/spf.pdf

4. It would be unduly burdensome to expect Government agencies to subdivide all counsel's briefs between the Restricted and Protect categories. (Protect is a less sensitive category than Restricted but defines personal material which must nevertheless be treated with care. It is not used by the Police who would always use Restricted). It is simpler to categorise as Restricted all information which is received by barristers within a brief or backsheet from a Prosecution or other Government agency for professional purposes and which they are required to treat as subject to a confidentiality obligation. In the absence of specific instructions from Instructing solicitors, these Guidelines apply to all such material received by barristers from Prosecution or other Government agencies for professional purposes and which barristers are required to treat as subject to a confidentiality obligation. Such information is referred to in these Guidelines as Restricted material even if it falls within the Government's classification Protect rather than Restricted and whether or not it is actually marked Restricted or Protect. It also applies to documents which Counsel creates.

5. These Guidelines are concerned only with Restricted material and focus upon:

A. the receipt and handling of physical material
B. the storage and handling of electronic material
C. electronic communications
D. the reporting of loss of data
E. the disposal and/or return of physical or electronic material.
F. material taken outside the UK

GUIDELINES

General Duties and Obligations

1. Barristers are reminded that it is the individual responsibility of barristers to preserve the confidentiality of the client's affairs and not without the prior consent of the client or as permitted by law to lend or reveal the contents of the papers in any instructions to or communicate to any third person (other than another barrister,[2] a pupil, or any other person who needs to know it for the performance of their duties) information which has been entrusted to him in confidence or use such information to the client's detriment or to his own or another client's advantage.[3]

2. You or Chambers should have an information risk policy setting out how to safeguard information in Chambers. You may adopt or adapt these Guidelines, or create your own policy. You or Chambers may be required to disclose the policy for the purposes of an annual audit.

A. The Receipt and Handling of Physical Material

3. *Restricted* material should never be left freely available in the clerks' room or in any other common area in chambers where it may be read by other members of chambers or visitors.

4. *Restricted* material should not be left in a position where it might be read inadvertently by another person entering the room.

5. *Restricted* material should never be read or worked on in public where it can be overlooked by members of the public.

6. *Restricted* material should be stored in Chambers or any other secure place to which the barrister instructed has regular access. A barrister may work on *Restricted* material at home provided that the material is put away when not in use.

7. Restricted material should be moved securely. On public transport Restricted material should not be left unattended. If travelling by private car, where practicable, keep it out of sight and stored as inconspicuously as possible. Restricted material should not be left in a car unattended except where the risk is less of a risk than taking it with you. It should never be left in a car overnight.

B. The Storage, Use and Handling of Electronic Material

---

[2] including, in the case of a registered European lawyer, the person with whom he is acting in conjunction for the purposes of paragraph 5(3) of the registered European Lawyers Rules: Rule 702 of the Code of Conduct (2009)

[3] Paragraph 702 of the Code of Conduct

8. Great care should be taken to ensure that that laptops, removable devices and removable storage media containing *Restricted* material are not lost or stolen. In particular:

   (a) such laptops and other removable devices should never be left unattended in public places or left in a car overnight (although they may be left unattended in a locked court during adjournments).

   (b) the material on any laptop or other removable device should be kept to the minimum necessary to enable work to be carried out efficiently.

9. The electronic storage of *Restricted* material requires certain minimum levels of security:

   (a) all computers used by counsel for work must be protected by up to date anti-virus and anti-spyware software, subjected to regular virus scans and protected by an appropriate firewall for the computer used. The operating software should be checked regularly to ensure that the latest security updates are downloaded. Access to all computers must be password protected.

   (b) particular care should be taken to avoid potential infection by malware, e.g. by downloading software other than from trusted sources.

   (c) work in progress should be regularly backed up, and back-up media used for *Restricted* material should be locked away if possible.

   (d) computers used for working on *Restricted* material at home should be protected from unauthorised and unrestricted access by third parties. Where practicable, the ideal is a computer linked to Chambers used only for Counsel's work.

   (e) wherever practicable, *Restricted* material stored on removable devices or removable storage media (such as memory sticks, CD-ROMs, removable hard disk drives and PDAs) and laptop computers must be encrypted to FIPS 140-2 or CCTM (CESG Claims Tested Mark) standards or to such other standards as may be approved by the professional client. Whole disc rather than folder encryption is required.

   (f) where the client provides its own removable devices or removable storage media, that should be used before using your own.

   (g) A decryption device or code created by counsel for the emergency recovery of encrypted material should be stored in a secure locked place such as a safe.

10. Reasonable steps should be taken to ensure the reliability of staff that have access to Chambers IT systems (including identity checks and references),

and encryption of particularly sensitive documents may be necessary to prevent technical staff accessing them. Staff in Chambers must have annual training on the importance of information security.

11. Chambers should make arrangements to create and maintain a log of all computers used by counsel for storing or working on *Restricted* material. The log should record the type, model and serial number of each computer used by counsel (other than dedicated thin-client terminals[4] or similar workstations provided by Chambers), together with the details and currency of any anti-virus, anti-spyware, encryption or other security software maintained on each machine.

12. Chambers should have procedures in place for the reporting of any loss of electronic *Restricted* material, computers, removable devices or removable storage media on which such material is or might be stored.

13. Wherever possible computers should not be placed so that their screens can be overlooked, especially when working in public places. It is recognised that this may not be possible in Court.

14. Passwords used to access computers or encrypted data should be at least 9 letters or more in length and should contain at least three out of the four keyboard symbols (upper case; lower case, numbers and symbols). Access by a fingerprint scanner is an acceptable alternative.

C. Electronic Communications

15. Counsel should use CJSM to send and receive RESTRICTED material by e mail.

16. Unless otherwise stated, counsel must assume that any Government Department or agency which sends emails under the CJSM system wishes to preserve the security of the material thus communicated. Accordingly, such emails cannot be forwarded, either manually or automatically, to other email addresses without the consent of the sender or the providers of the service. Such emails may be safely retrieved from other computers over the internet through Virtual Private Networks (VPNs).

23 Attachments containing *Restricted* material may be sent unencrypted via CJSM emails. Such attachments may only be sent by other email systems if the material is encrypted to FIPS 140-2 standards or to such others standards as may be approved by the relevant Department or Agency.

24 Passwords required to decrypt an email attachment must never be sent in the same email as the encrypted attachment.

---

[4] A dedicated thin client terminal sends keyboard and mouse input to the server and receives screen output in return: it only processes the user interface (UI) and does not process any data. Data is stored on the Chambers server.

D. Reporting of Loss of Data and Minimising Consequential Risks

25. Accidents happen and thefts occur. Where *Restricted* material is lost the professional client, Chambers and, where appropriate, the police must be informed as soon as possible.

E. The Disposal of Physical or Electronic Material.

26. *Restricted* material should not be retained in electronic form when it is no longer required. For the avoidance of doubt, counsel may retain anonymised precedents, pleadings and advices and any documents which have been deployed publicly in open court.

27. All Chambers should have systems in place for the secure disposal of *Restricted* material i.e. the cross cut shredding of papers and CD ROMs.

28. Any *Restricted* material disposed of by counsel must be disposed of by using a secure method of disposal.

29. Counsel who wishes to dispose of any computer, hard drive, removable drives or other removable media on which *Restricted* material has been stored, including computers used at home, must ensure that the relevant media is effectively destroyed or wiped before disposal using a recognised method to ensure that information is put beyond recovery. Mere file deletion, single pass overwriting or reformatting is insufficient. Physical destruction or the use of specialist deletion and overwriting software is required.

30. Departments may require confirmation that *Restricted* material has been returned or destroyed securely.

F. Material taken outside the UK

31. (1) No hard copy Restricted material may be taken outside the UK without prior permission from the instructing Government department or Agency concerned.

(2) Subject to (3) below, no encrypted Restricted data may be taken outside the UK on any memory stick, USB stick, CD, DVD or any other small portable storage device without prior permission from the instructing Government department or Agency concerned.

(3) Encrypted Restricted data that ***does not relate to*** **cases involving national security or which does not originate from the Serious Organised Crime Agency** may be taken outside the UK on an encrypted laptop provided regard

is had to paragraph 8(b) (keeping material to the minimum necessary to enable work to be carried out efficiently).

(4) Counsel are reminded that no material which falls within any higher security classification than Restricted (e.g. Confidential, Secret, Top Secret) may be removed from the UK in any circumstances without the express permission of the Government Department or Agency concerned. Such material should, not of course, be being kept on Counsel's laptops and other portable storage device in any event.