GUIDELINES for COUNSEL

On

INFORMATION SECURITY

And

GOVERNMENT WORK

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 Counsel should take to meet the particular requirements of the United Kingdom Government, the Scottish Government and any of their respective agencies ("both Governments"). They have been prepared by the Government Legal Service Scotland ("GLSS") who represent those interests in conjunction with the Faculty of Advocates ("the Faculty"). Although they do not apply to information provided to Counsel by other clients, you are requested to have these Guidelines in mind when dealing with Restricted information which may have originated from both Governments.

Categories of information

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

(a) Many documents routinely supplied to counsel acting for both Governments 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 parties, or witnesses. The data may also provide information concerning current investigations.

(b) Both Governments 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, 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, or relevant department in either Government. 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 [UK] Government Departments provide counsel with safes, secure dedicated laptops, photocopier 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.

4. It would be unduly burdensome to expect both Governments to subdivide all Counsel's brief between the Restricted and Protect categories. (Protect is a less sensitive category than Restricted but defines personal material which must nevertheless be treated

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

with care). It is simpler to categorise as Restricted all information which is received by Counsel in the form of instructions 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 Counsel from either Government for professional purposes and which Counsel 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 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. Counsel are reminded that it is the individual responsibility of Counsel to preserve the confidentiality of the client's affairs. This should only be waived with the prior consent of the client or as permitted by law. That includes lending or revealing the contents of papers or instructions, or to communicate to any third person (other than another Counsel,[2] a Devil, or any other person who needs to know it for the performance of their duties) information which has been entrusted in confidence or use such information to the client's detriment or to his own or another client's advantage.[3]

2. The Faculty will maintain an information risk policy setting out how to safeguard information within the Faculty. The Faculty 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 anywhere within the Faculty where it may be read by other members of Faculty, employees of the Faculty or visitors to the Faculty.

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

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 a secure place. Counsel 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

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

---

[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] "Guide to the Professional Conduct of Advocates"; 2008, at paragraph 2.3. See. http://www.advocates.org.uk/profession/index.html.

(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 a 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, 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, eg 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 the Faculty IT system 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 Faculty IT systems (including identity checks and references), and encryption of particularly sensitive documents may be necessary to prevent technical staff accessing them. Staff in the Faculty (including each Stable) must have annual training on the importance of information security.

11. The Faculty 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 the Faculty), together with the details and currency of any anti-virus, anti-spyware, encryption or other security software maintained on each machine.

12. The Faculty 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 the security of any material received in any e-mail from either Government via the CJSM system must be preserved. Accordingly, such e-mails cannot be forwarded, either manually or automatically, to other e-mail addresses without the consent of the sender or the providers of the service. Such e-mails may be safely retrieved from other computers over the internet through Virtual Private Networks (VPNs).

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

18. Passwords required to decrypt an e-mail attachment must never be sent in the same e-mail as the encrypted attachment.

D. Reporting of Loss of Data and Minimising Consequential Risks

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

E. The Disposal of Physical or Electronic Material

20. *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,

[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 Faculty server.

pleadings and advices and any documents which have been deployed publicly in open court.

21. The Faculty, (including each Stable) should have systems in place for the secure disposal of *Restricted* material ie the cross cut shredding of papers and CD ROMs.

22. Any *Restricted* material disposed of by Counsel must be disposed of by using a secure method of disposal.

23. Counsel who wish 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.

24. Either Government may require confirmation that *Restricted* material has been returned or destroyed securely.

F. Material taken outside the UK (Counsel representing the UK Government only)

25. (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* (eg 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.