The Baha Mousa Public Inquiry

Inquiry Chairman: The Right Honourable Sir William Gage

Security Policy*

Introduction

1. This policy outlines the procedures that should be maintained by all members of staff (permanent or contractors) to ensure that the Inquiry's premises and information are protected from accidental and malicious threats that could disrupt our business.

2. The document is divided into three sections, covering general office security, information security and the specific provisions that will be in place on days that the hearing centre is open for business. Please familiarise yourself with all sections, because we are all responsible for assuring the safety and security of our physical and information assets and our colleagues. In particular you should make yourself aware of the differences in security procedures between hearing and non-hearing days.

3. While Finlaison House and the Baha Mousa Public Inquiry are low risk targets, due to the location of Finlaison House we must constantly be aware of the dangers of malicious parties and report any suspicions that we have immediately to the building's security team..

4. Signs are displayed at the front & back of the building showing the present 'Response Level' that is required to protect the building and its contents from terrorist attack. The Response Levels which are laid down by the Home Office, are expressed as, Normal, Heightened and Exceptional. Security measures are increased as the Response Level Rises. They are set by security practitioners in Government. They are informed by the threat level but also take into account specific assessments of vulnerability and risk:

    - **Normal:** Routine protective security measures appropriate to the business concerned.
    - **Heightened:** Additional and sustainable protective security measures reflecting the broad nature of the threat combined with specific business and geographical vulnerabilities and judgments on acceptable risk.
    - **Exceptional:** Maximum protective security measures to meet specific threats and to minimise vulnerability and risk.

5. Please note that this Security Policy applies while the threat to the Inquiry is assessed by MOD as LOW. It might be changed from time to time, and any increase in threat assessment may lead to new procedures being adopted.

* This Security Policy has been abridged for publication. Some information contained within the original document has been removed to protect the personal data or health and safety of those involved in the Inquiry, including those who attend hearings, and/or to prevent crime or ensure the administration of justice.

Office security

Entry to the building and office

6. The Government Actuary's Department (GAD) are our landlords and are responsible for entry and security provisions. Entry to the building is by proximity pass. You must present your proximity pass and enter your PIN to enter reception, and you should wear your pass at all times when inside the building. If you forget your pass or your pin you will need to inform Finlaison House reception immediately. Please do not wear your pass outside the building, nor discuss any aspects of the building's security outside or with visitors to the building.

7. The office doors on Floors 3 and 4 have swipe locks which are activated by proximity passes. You must ensure the office door is closed and locked at all times. If you are the last person to leave the office, ensure that the door is locked closed behind you. The same is true for the common areas in the basement of the building.

8. There is always one security guard on duty within Finlaison House. They can be contacted via the reception helpdesk and are responsible for ensuring that the building is safe and secure at all times.

9. We must beware of "tailgaters" entering the building or designated office areas within the building behind others. If you are concerned, please challenge the individual to show their pass and contact reception if you consider a breach of security has occurred.

10. There follow some simple instructions to ensure that everyone does their bit to ensure the proper physical security of Finlaison House and the Inquiry:

Do -

- Remember your pass, show it on entering the building and wear it at all times when within the building.
- Let reception know in advance of any planned visitors and escort your visitors at all times
- Report anything suspicious either inside or outside the building

Don't –

- Let anyone tailgate into the building or onto any designated floor.
- Wait for others to report that someone is in the building or floor who clearly should not be.
- Go home until you have locked away all classified or 'business sensitive' documents, turned your PC off and placed all your keys in the box safes.

11. The building is open from 7am to 10pm during the week and 9am to 5pm on Saturdays. It is not normally open on Sundays. If you wish to work outside these hours we will need to pay for additional security provision. A week's notice is normally required to ensure access outside normal hours.

12. At the weekend there will only ever be one member of security staff in the building to cover reception and the rest of the building. Proximity pass access is disabled and the security guard on duty will let you in. If you intend to work over the weekend you will need to inform security *in advance* so that they can ensure that someone is available to let you in. Please be aware of the reduced security cover in implementing any of the procedures contained in this policy.

Visitors

13. Because the Inquiry is located within a secure building, the reception must be informed of all visitors in advance. This is done by a simple email to gadreception@gad.gov.uk detailing the name(s), date and time of arrival.

14. When reception notifies us that a visitor has arrived, they will issue a visitor pass for the building, and direct the visitor to the reception waiting area. A member of the team will then collect the visitor. The Inquiry is responsible for the safety and behaviour of the visitor. At no point should visitors be left unattended within the building: they must be escorted at all times. When the visitor departs their visitor pass for the building must be handed in to reception.

Clear Desk Policy

15. The Baha Mousa Inquiry operates a clear desk policy. At the end of each day all files must be returned to the relevant cabinet and other papers either to the safe or to a locked cupboard as appropriate. This means that when you are not in the office there should be no papers or files (including electronic media containing files) on your desk. All 'in trays' and similar containing papers must be locked away when you leave the office. It is your responsibility to ensure a clear and tidy workplace.

16. The areas around printers, copier, fax machine, scanner, etc. must be kept free of paper. Printing or copying not required should be shredded and spare printing paper that will not fit into any of the machines returned to the relevant stationery cupboard.

17. For more information on information security, including the storage, transmission and destruction of classified information, please see the next section of this policy.

Vigilance

18. We are all responsible for keeping an eye open for risks to our business. Physical risks include water damage, fire and bomb threats. In all cases we should act quickly when a threat, or potential threat, becomes apparent.

19. In the event of a non-emergency, please alert the appropriate people quickly, starting with the Inquiry Secretariat who should be able to liaise with whoever else might need to be involved.

20. **If you discover a fire**, raise the alarm by breaking the glass at the nearest fire alarm call point. Personal safety is the priority. In all but the most minor incidents, you should leave the fire fighting to the professionals. Fire Marshals are designated for all areas of the building and they will have made themselves aware of anyone within

their area with special needs. The members of staff requiring assistance should be escorted to the nearest fire exit and assisted to safety or accompanied to the nearest Refuge Point. The fire warden should pass on information regarding the location of any persons requiring assistance when they make their report to the Incident Control Office.

21. The Fire Marshals include Frances Currie for the 4th floor and Ben Connah for the 3rd floor. The Fire Evacuation Procedure is contained in the Inquiry's *Hearing Arrangements* leaflet at Annex A which is distributed to visitors to the Inquiry [but has been removed from this document for security reasons].

22. **If you discover a bomb or suspect package,** tell the senior person in your area and together you should evacuate entire floor to the west wing stair well (stair well 2) which has been designated as a safe area. Inform Reception immediately, who will inform the appropriate people within the building. Wait for instructions to evacuate the building. Do not leave the building unless there is no alternative.

23. Further detail on bomb safety procedure is contained at Annex B [which has been removed from this document for security reasons], along with specific instructions relating to postal threats. Always remember:

- DO NOT touch any suspicious object;
- DO report it to the security team immediately via Reception;
- DO NOT ignore any suspicious object.

24. Please note that THE EMERGENCY EVACUATION PROCEDURE IS SIGNALLED BY A CONTINUOUS ALARM. It is tested every Thursday and the test will; be announced in advance. At all other times we should evacuate the building IMMEDIATELY on hearing the alarm.

Information security

Information and communication technology

25. As part of the Cabinet Secretary's Review of Data Handling in Government, all employees who process information on behalf of a Government department need to be familiar with the procedures surrounding information security.

26. All information will either be held electronically or in hard copy. Certain standards must be adhered to for classified material and these are outlined below, but there are also some common sense measures that we can take to ensure that our electronic systems are as secure as they need to be.

27. All computers should be password protected with a password known only to the user. Change your password regularly; especially if you suspect that someone else might have become aware of it.

28. When using the shared drive to store and view work, ensure that you do not delete anything without the express consent of the document's originator. For classified material (up to Restricted) you should apply a password to information so that it is not freely available. Information above Restricted should NEVER be held on our electronic network or hardware.

29. There is a dedicated laptop for viewing classified material above Restricted. It should only be used as a stand-alone, and should not be connected to any of the Inquiry's systems except a non-networked printer if necessary.

30. All laptops that are used to store, edit or process any Inquiry information must be encrypted, and any portable media (CDs, USB sticks, portable hard drives) must be encrypted if they contain information classified above Restricted or if they contain many datasets (say more than 1,000) classified Protect or Restricted.

31. If you have any doubt about whether you can use your IT systems in certain ways and with certain types of material, please refer to Frances Currie in the first instance.

Handling information with protective markings

32. Most information we handle should be unclassified. This information may be sent to others by e-mail, or through the post. But it should be kept out of sight at night (remember the clear desk policy) and even though it is unclassified, it is not published material and care should be taken to ensure that it is not seen by people outside the Inquiry.

33. Many Government documents have protective markings. This section explains what those markings are and sets out how to handle information with protective markings.

34. There are five levels of protective marking. These are:

- TOP SECRET

- SECRET
- CONFIDENTIAL
- RESTRICTED
- PROTECT

35. All five can be applied to international relations, defence, public order and civil rights, and economics.

36. The three that we are most likely to use or to handle are documents marked Confidential, Restricted or Protect and these apply to economic interests, defence, law enforcement and policy and operations of public service.

37. There may be some documents with the SECRET marking that come into the office though some of these may have been declassified before circulation to the Inquiry.

Storage of protectively marked documents – up to SECRET

38. PROTECT or RESTRICTED information should not be shown to people other than those who are specifically entitled to see it. This should be self evident from the status of the document, but please seek advice if you are uncertain. Please note that it may well be that documents classified in this way should not be seen by others within the Inquiry team.

39. CONFIDENTIAL documents must be kept in security containers at all times they are not in use. They must not be sent by e-mail, neither must they be scanned into the database. If you wish to send a CONFIDENTIAL document to someone outside the building, please contact the Secretariat who will arrange for secure delivery, which will depend on the amount of material to be sent and the location of the recipient. If we receive CONFIDENTIAL or SECRET information in electronic format, we must only use a stand-alone laptop to view the information, and we must be sure that the laptop will never in future be connected to any network. There is a laptop in the safe for this purpose and it should be treated like any other asset classified as SECRET.

40. SECRET documents must be kept in the safe at all times when they are not in use. Such documents must be logged in and out of the safe using the document log (MoD Form 102). SECRET documents must not be circulated by post, copied, scanned into the database or sent by fax. If additional copies are needed, please contact either the Solicitor to the Inquiry or the Secretary to the Inquiry. On no account must SECRET material be held anywhere but in the safe.

41. Unfortunately we are receiving quite a lot of material from other sources where it is not immediately clear whether the information is classified. This is mainly evidence bundles and the status of individual documents become clear as it is checked for scanning. Until we are clear as to the status of any file of documents, please treat it as CONFIDENTIAL. Once the precise status of a document has been established it can then be treated according to that status.

42. We also receive documents electronically. If a CD or USB stick, for example, contains classified material it must be marked as such and treated accordingly.

43. We can declassify or downgrade a lot of the material we receive, but this must be done properly, either by the Solicitor to the Inquiry or by the Secretary to the Inquiry, and after consultation if necessary with the originator of the document. Please ask if you think a document ought to be declassified or have a lower classification than indicated.

Sending protectively marked documents – up to SECRET

44. Protective markings should not appear on the outside of any envelope, packaging or container sent outside the Inquiry.

45. Special restrictions apply to documents with protective markings being sent abroad and where it is necessary to send documents out of the UK this should first be discussed with the Inquiry Security Controller (Lee Hughes) or his assistant (Frances Currie).

46. Contract details for transporting documents and files within the UK are set out in the Office Manual.

47. Documents Marked RESTRICTED should be mailed in a sealed double envelope after confirming correct full postal address including post code. Sender details must be on the inner envelope and you must ensure the recipient is expecting the letter or package. The cover must not be marked with a protective marking, caveat or descriptor, other than PERSONAL or ADDRESSEE ONLY. It should be addressed to an individual by name or appointment (including full address and post code).

48. Documents Marked CONFIDENTIAL can be sent by trusted hand in a sealed cover or secured container or, by post or other courier or messenger service, in which case the following applies:

    - a single cover (government addresses only) must not be marked with the protective marking, caveat or descriptor, other than PERSONAL or ADDRESSEE ONLY, and must be addressed to an individual by name or appointment (including full address and post code);
    - double covers must be used if sent to a non-government address, marked and addressed as described below. Outer covers should not show the protective marking but must show the recipients name, appointment and full address (including postcode), and the following return address in the event that delivery cannot be made: PO Box 64355, London EC1P 1PN.

    Inner covers should be similarly addressed, clearly marked CONFIDENTIAL.

49. Documents Marked SECRET are to be carried only by a trusted individual, approved courier, Parcelforce 10, 11, 12 or 24 hour service for envelopes, boxes and large or heavy packages, or Royal Mail Special Delivery Services in secured container or double cover. Where carried by commercial courier or postal service receipts (MOD Form 24) are required as proof of delivery.

50. The outer cover must not be marked with the protective marking but must show the recipients name, appointment and full address (including postcode), and the

following return address in the event that delivery cannot be made: PO Box 64355, London EC1P 1PN.

51. The inner cover must be similarly addressed, clearly marked SECRET. A receipt (MOD Form 24) is to be inserted with the document before sealing.

Transporting documents and files with markings up to SECRET

52. We have a contract through MOD with Parcelforce to transport boxes for the Inquiry on a 10, 11, 12 or 24 hour service. They will deliver to the named contact only so ensure that the person whose name is on any boxes, etc. will be in the building when the delivery is likely to be made.

53. Documents for immediate delivery should be taken by a trusted messenger/member of staff in a taxi for delivery to the named contact only. Please ensure they will be there when the messenger arrives. To arrange a taxi for this call Dial-a-Cab – details are in the Office Manual.

Sending documents via electronic media

54. Restricted and Protect documents may be sent by e-mail to other email addresses that are capable of receiving secure email. In effect this means anyone else with access to the Government Secure Intranet (GSI) or, less likely, the Criminal Justice Secure e-Mail server (CJSM). To send secure email from Inquiry email accounts simply add ".cjsm.net" to the end of an email address.

55. If you need to send information on removable media (such as CD/DVD) the information should be encrypted and password protected; file names should not give an indication of the information held. Information should not be sent out on USB sticks.

56. Nothing above RESTRICTED should be sent via electronic media.

Sending documents via fax

57. When sending PROTECT documents by fax, the recipient must be contacted and be standing by the fax to receive it/them. RESTRICTED, CONFIDENTIAL or SECRET documents are not to be faxed.

Disposal of papers

58. Anything with a protective marking should be shredded using the cross cut shredder.

Disposal of electronic media

59. All CD/DVD/floppy disks with a protective marking must be shredded on site by using the relevant part of the shredding machine. System data and hard drives require specialist disposal contact Frances Currie or the Help Desk.

Discussion by telephone (landline, mobile or video conference)

60. There should not be discussion of RESTRICTED material or above by telephone.

Working at home or when travelling

61. It is not permitted to remove classified documents from the office to use for work at home or when travelling unless they are contained on an encrypted laptop. Note that no information classified above RESTRICTED may be held electronically, which means that no information CONFIDENTIAL or above should be removed for work in transit or at home.

Security on hearing days

62. On hearing days, the swipe entry mechanism will be disabled to allow access to legal teams, public and press. All of us must be vigilant to abuse of this, and we should remember that we are not the only organisation in the building whose work and information might be of interest to outside individuals and groups. The Inquiry team has worked closely with City of London police, GAD and MITIE Security (GAD's security supplier) to ensure that the building remains as secure as possible consistent with the efficient running of the Inquiry.

Entry to the building

63. On hearing days additional security staff will be in place on the hearing days and anyone wishing to enter the building who does not have a valid Finlaison House pass will be subject to a standard bag search and body scan (a hand held metal detector or 'security wand' is used in this instance). The only exception will be for visitors to Finlaison House who have planned in advance to see Inquiry (or GAD/HTA) staff separately from the hearing. In this instance visitors will need to report to reception and be collected and escorted at all times in the usual way.

64. To avoid disruption for pass holders, the reception area will be divided in half and pass holders can enter on the right-hand side, showing their pass to the guard/receptionist in the usual way. Non-pass holders will enter on the left side and a separate reception desk will conduct searches and issue day passes.

65. To avoid congestion in reception, visitors to the Inquiry will be asked to queue in Took's Court. They will be ushered into the building in small groups where they will be searched and issued with the appropriate badge (legal, press, public or participant) and onwards into the left-hand lift. On hearing days this lift will be taken out of regular service to ensure that members of the public and press can only exit at Floor 3. The Inquiry will ensure that there are sufficient ushers to marshal all attendees. In the event of an emergency rigorous evacuation procedures will be followed and re-entry to the building will be exactly as described above.

66. Legal teams may wish to access the hearing room to deposit papers etc. If so, they can do so only on the day of the hearing in question and will not be able to leave

papers in the room overnight. The double doors to the hearing room will be locked whenever papers are inside until 8:30am on the morning of hearings and from half an hour after the hearing has closed. Participants may leave papers in dedicated locked cabinets in the consulting rooms, and they will be entrusted with the keys to these. All keys to locks on Floor 3 are held in the key box under the receptionist's desk. The key to that box is held in the main key box on Floor 4. The Hearing receptionist will generally be responsible for allocating and logging keys. In her absence Ben Connah is responsible

During hearings

67. Security staff will be in attendance throughout the day. Someone, either the receptionist or a guard, will be situated at the main door to Floor 3 and will monitor anyone coming in or out, ensuring that they have the correct badge and that they know where to sit. In the hearing room an usher will be responsible for receiving anyone from the reception area and seating them quietly in the correct place.

68. As people come and go, security and the receptionist will be responsible for informing each other about movements within the building to ensure that no-one can wander off to explore. So if someone exits Floor 3 using the stairs, the receptionist will radio ground floor security to inform them to expect someone in the stairwell. Likewise the lifts.

69. Anyone leaving the building, for however little time will undergo the same security checks when they re-enter.

70. There is a limit of 20 members of the public at any one time, but this can be extended if there is sufficient space in the overspill or press areas at the discretion of the Secretary or Deputy Secretary only.

Roles and responsibilities

71. The Secretariat is responsible for ensuring that sufficient resource is dedicated to the orderly entry of visitors and to managing their movements when inside the building. We will ensure that there are individuals in ground floor reception, in the lift and on Floor 3 in the reception area and press and hearing rooms. In the event of evacuation, the Inquiry's fire marshals and hearing room staff will shepherd people out of the building. In order to ensure full coverage it may from time-to-time be necessary for members of the Inquiry team to take on these roles, or for members of the security or buildings management teams to take on duties generally undertaken by Inquiry staff. Ben Connah is responsible for these arrangements and any queries about them should be directed to him in the first instance.

For more general security issues, Frances Currie should be the first port of call as the Inquiry's Deputy Security Co-ordinator.

The Baha Mousa Public Inquiry

Inquiry Chairman: The Right Honourable Sir William Gage

Annex A: Hearing arrangements

GENERAL SAFETY

Inquiry attendees are asked to note the following:

- Be alert to general aspects of health and safety
- Accidents or illness must be reported to a member of Inquiry staff
- If you require help whilst in Finlaison House or assistance with any aspect of health and safety please speak to a member of staff
- Please display your entry badge prominently at all times

HEARING ROOM ETIQUETTE

The public are welcome to attend hearings and are asked to follow certain standards of behaviour:

- There must be silence in the public gallery while the Inquiry is sitting. Please do not enter or leave the hearing room during proceedings
- As in courts of law the use of mobile telephones, blackberries, recording equipment, cameras and personal stereos is strictly prohibited, so please ensure such equipment is turned off before entering the room
- The consumption of food and drink is not permitted in the hearing room

The Baha Mousa Public Inquiry

Inquiry Chairman: The Right Honourable Sir William Gage

HEARING ARRANGEMENTS

- **Emergency procedure**
- **General safety**
- **Hearing room etiquette**

Welcome to the Baha Mousa Public Inquiry. Please read this leaflet carefully for your own safety and comfort whilst attending the hearing

If you have any questions, please contact the Inquiry reception desk next to the lift on the 3rd floor

[After advice from the City of London police we have removed from this document details of our fire evacuation and bomb threat procedures. This is done by reference to sections 31 (prevention of crime) and 38 (health and safety) of the Freedom of Information Act 2005]