OMAGH
BOMBING INQUIRY

OPERATIONALLY SENSITIVE MATERIAL RESTRICTION ORDER

("OSRO")

RESTRICTION ORDER PURSUANT TO SECTION 19 OF THE INQUIRIES ACT 2005

This Restriction Order is made pursuant to section 19(1) of the Inquiries Act 2005 ('the Act').

Any threat to break such an order, or any breach of it, can be certified to the High Court or Court of Session under section 36 of the Act, and the Court will deal with it as though the breach had occurred in proceedings before that Court.

IT IS ORDERED THAT:

A: General

1. This Operationally Sensitive Restriction Order (the OSRO) is made on 13 January 2026 and remains in force indefinitely.

2. The Chairman may vary or revoke the OSRO by making a further order at any point.

3. Any breach of the OSRO by any means whatsoever shall be notified in writing to the Solicitor to the Inquiry immediately upon identification of the breach.

4. For the purpose of this OSRO, Operationally Sensitive Material (OS Material) is material that has been identified to fall within either of the two OSRO categories specified in Annex A to this OSRO.

5. No person may reveal, disclose, share or publish anything that has been identified as OS Material or the substance of it, save as provided for by the ORSO.

6. References to 'the Inquiry' are to the Omagh Bombing Inquiry.

B: OS Files

7. Computer files containing OS Material will be disclosed to Core Participants in two formats:

    a. **OPEN –** The open version of these files is redacted to obscure OS Material (the Open File), in addition to any redactions applied for reasons outside the scope of this Order. The reason for each redaction is specified in the document. OS Material redacted under the OSRO is overwritten with "OS". The Open Files are disclosed on the Relativity Disclosure System in a database entitled 'Omagh Bombing Inquiry - Core Participants' (the Open Database).

    b. **OPERATIONALLY SENSITIVE** – The operationally sensitive version of these documents (the OS File) contains visible OS Material. The OS Files are disclosed on the Relativity Disclosure System in a database entitled 'Omagh Bombing Inquiry - OPERATIONALLY SENSITIVE' ('the Operationally Sensitive Database').

8. The files included in the Operationally Sensitive Database and the equivalent Open File may be varied at any time by the Chairman.

9. Save for the OS Material in them, the Open Files are not restricted by the OSRO.

10. The OSRO does not prohibit:

    a. The disclosure of OS Material by a Material Provider to the Inquiry Legal Team as part of the disclosure process; or

    b. The disclosure of OS Material by the Inquiry Legal Team to any 'Authorised Person', as defined at paragraph 11.

C: Access to the OS Files

11. Access to the Operationally Sensitive Database is restricted to the following 'Authorised Persons':

    a. The Chairman;

    b. The Inquiry Legal Team, comprising:

        i. Counsel to the Inquiry, as defined by rule 2 of the Inquiry Rules 2006;

        ii. Solicitor to the Inquiry, as defined by rule 2 of the Inquiry Rules 2006, and

        iii. Solicitors, paralegals or junior counsel instructed or employed by or on behalf of the Solicitor to the Inquiry for the purpose of assisting the Chairman to discharge the Inquiry's terms of reference.

    c. The Secretary to the Inquiry, as defined by rule 2 of the Inquiry Rules 2006, and any member of the Inquiry Secretariat.

    d. Experts instructed by the Solicitor to the Inquiry who require such access in order to fulfil their instructions;

    e. Any person instructed by the Solicitor to the Inquiry to create presentational materials for the purpose of the Inquiry's oral evidence hearings;

    f. Core Participants, as defined by rule 2 and rule 5 of the Inquiry Rules 2006. Where the Core Participant is an organisation or public body, this means the individual / individuals acting as their client whose name(s) and role(s) have been identified to Solicitor to the Inquiry in writing;

g. Recognised Legal Representatives, as defined by rule 2 and rule 7 of the Inquiry Rules 2006;

h. Subject to paragraph 12b, those working for or instructed by an RLR on behalf of a Core Participant;

i. Any witness the Chairman considers needs to see the OS File for the purpose of their evidence to the Inquiry;

j. Any other person the Chairman determines should be provided with access.

12. The Operationally Sensitive Database is subject to the following requirements:

a. The sharing of Relativity access to the Operationally Sensitive Database with any person other than an Authorised Person for any reason whatsoever is prohibited.

b. Recognised Legal Representatives must notify the Solicitor to the Inquiry in writing of the names of those persons listed at paragraph 11f and 11h that require access to the Operationally Sensitive Database. Written authorisation from the Chairman is required before such a person is permitted access to the Operationally Sensitive Database.

c. All those identified at paragraph 11d to 11j granted access to the Operationally Sensitive Database must, where required to do so, have returned a signed copy of the Inquiry's Confidentiality Undertaking to the Solicitor to the Inquiry before they shall be permitted access to it.

d. Save as set out at paragraph 12e, the OS Files and/or their content must not be printed, downloaded, copied, photographed or otherwise replicated or saved, whether in full or in part, by any means whatsoever.

e. Paragraph 12d does not apply to the Chairman or those persons listed at paragraph 11b, 11c and/or 11d when acting to assist the Chairman to discharge the Inquiry's terms of reference.

f. The Operationally Sensitive Database shall not be accessed / viewed on a mobile phone or tablet device.

g. The Operationally Sensitive Database shall not be accessed / viewed in a public place. For the purpose of this paragraph, the Inquiry hearing room and in conference rooms / meeting rooms at the Inquiry hearing venue are not a public place.

h. When viewed in a private place, precautions must be taken to ensure that there is no risk of someone who is not an Authorised Person viewing any material on the Operationally Sensitive Database.

D. Use of the OS Files

13. The content and/or substance of OS Files may be dealt with in the following ways:

a. Authorised Persons can refer to the content and/or substance of OS Files at an Operationally Sensitive Restricted Hearing.

b. An Authorised Person can show the content of an OS File to another Authorised Person in relation to and/or for the purpose of assisting the Chairman to discharge the Inquiry's terms of reference. Where the Authorised Person is an organisation or public body, the Authorised Person can show the content of OS Files to the individual / individuals acting as their client whose name(s) and role(s) have been identified to Solicitor to the Inquiry in writing, subject to each person having signed and returned to the Inquiry a confidentiality undertaking. The showing of the content of an OS File is subject to the restriction and precautions set out at paragraph 12g and h.

c. The Inquiry Legal Team, as defined by paragraph 11b, can show members of the accredited media the content of an OS File in accordance with paragraph 31.

d. Authorised Persons are permitted to discuss the content and/or substance of OS Files with other Authorised Persons who have signed and returned a confidentiality undertaking to the Inquiry where such discussion is related to and/or for the purposes of assisting the Chairman discharge the Inquiry's terms of reference. Strict precautions, including by way of conducting any conversation in private and the use of robust digital security, must be taken when discussing or sharing the content or substance of the OS Files.

14. An Authorised Person may request permission from the Chairman to show the content of OS Files to a named person who is not an Authorised Person. Written authorisation from the Chairman must have been received in advance of showing the content of OS Files to such a person. The named person wishing to view OS Files must, where required to do so, have returned a signed copy of the Inquiry's confidentiality undertaking to the Solicitor to the Inquiry before they shall be permitted access to it.

E. Operationally Sensitive Restricted Hearings

15. Any hearing held for the purpose of receiving oral and/or written evidence containing or otherwise referencing OS Material will be referred to as an Operationally Sensitive Restricted Hearing ('OSRH').

16. Evidence received at an OSRH, whether oral or documentary, will be referred to as Operationally Sensitive Evidence ('OS Evidence').

17. The following people shall be permitted to attend an OSRH:

a. Any Authorised Person;

b. Any witness or expert giving evidence relevant to the OS Material under consideration at the OSRH while giving evidence and during such further part of the OSRH as they are given permission by the Chairman to attend;

c. Any person performing functions necessary for the proper functioning of the OSRH, including a stenographer, usher or AV operator;

d. Any accredited member of the media;

e. Any other person the Chairman expressly authorises to attend.

18. Paragraph 17 is subject to the Chairman's discretion to exclude any person whom he considers should not be permitted to attend.

19. There shall be no public broadcast of the OSRH.

20. There shall be no private broadcast of the OSRH to any Authorised Persons save the Inquiry Legal Team, as defined by paragraph 11b.

21. There shall be a livestream of the OSRH to the remote hearing room in Omagh. All requirements under this OSRO which apply to the OSRH will apply to the remote hearing room in Omagh and those there present during the livestream of an OSRH.

22. The substance of OS Evidence may not be repeated or otherwise communicated in any way outside the OSRH, or any subsequent OSRH, save as provided for by this OSRO.

23. At the conclusion of the OSRO the Chairman may, of his own motion, direct that the OSRO is lifted over any or all OS Evidence.

24. An opportunity will be given at the conclusion of an OSRH for any attendee to apply to lift the OSRO over any or all OS Evidence, and for any other attendee to oppose such an application.

25. At any other time, whether of his own motion or upon application, the Chairman may lift the OSRO in relation to any or all OS Evidence.

26. In the event the Chairman lifts the OSRO of his own motion or upon application in the circumstances set out at paragraphs 23, 24 and 25 above, that evidence will cease to be OS Evidence and can be repeated, reported or otherwise communicated without any restriction.

27. A transcript of any part of the OSRH in relation to which the Chairman has lifted the OSRO will be published on the Inquiry's website. No other part of the transcript for an OSRH will be published on the Inquiry's website.

28. A transcript of any part of an OSRH not published on the Inquiry's website will be available to Authorised Persons on the Operationally Sensitive Database, subject to the restrictions applying to the Operationally Sensitive Database and OS Files as set out at paragraphs 12 and 13.

29. Any document displayed during an OSRH in relation to which the Chairman has lifted the OSRO will be published on the Inquiry's website. No other OS File displayed during an OSRH will be published on the Inquiry's website.

30. Any document or other file displayed at an OSRH but not published on the Inquiry's website will be available to Authorised Persons on the Operationally Sensitive Database, subject to the restrictions applying to the Operationally Sensitive Database and OS Files as set out at paragraphs 12 and 13.

31. Accredited members of the media may apply at any time to inspect:

    a. any document or other file displayed during an OSRH but not published on the Inquiry's website; and/or,

    b. the transcript of any part of an OSRH not published on the Inquiry's website.

Any accredited member of the media permitted to see such transcripts, documents or files will be subject to the restriction at paragraph 22 in relation to the content.

32. The restriction at paragraph 22 does not apply to Authorised Persons, provided the OS Evidence is dealt with in accordance with the precautions set out at paragraph 13b above.

PENAL NOTICE

33. The High Court and the Court of Session have the power to imprison or fine for any breach of this Order.

13 January 2026

OPERATIONALLY SENSITIVE MATERIAL RESTRICTION ORDER

("OSRO")

ANNEX A

OSRO Category A	Tactics and capabilities used by the UK state authorities and others in the investigation and/or disruption of suspected terrorist or other criminal activities.
OSRO Category B	Methods and strategies used by individuals in the preparation and /or commission of suspected terrorist or other criminal activities.